

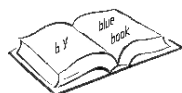
il MATEMATICO *e il* DETECTIVE

COME I NUMERI POSSONO RISOLVERE UN CASO POLIZIESCO

di

KEITH DEVLIN e GARY LORDEN

Traduzione di ELISA FARAVELLI



PROPRIETÀ LETTERARIA RISERVATA

Longanesi & C. © 2008 - Milano

Gruppo editoriale Mauri Spagnai

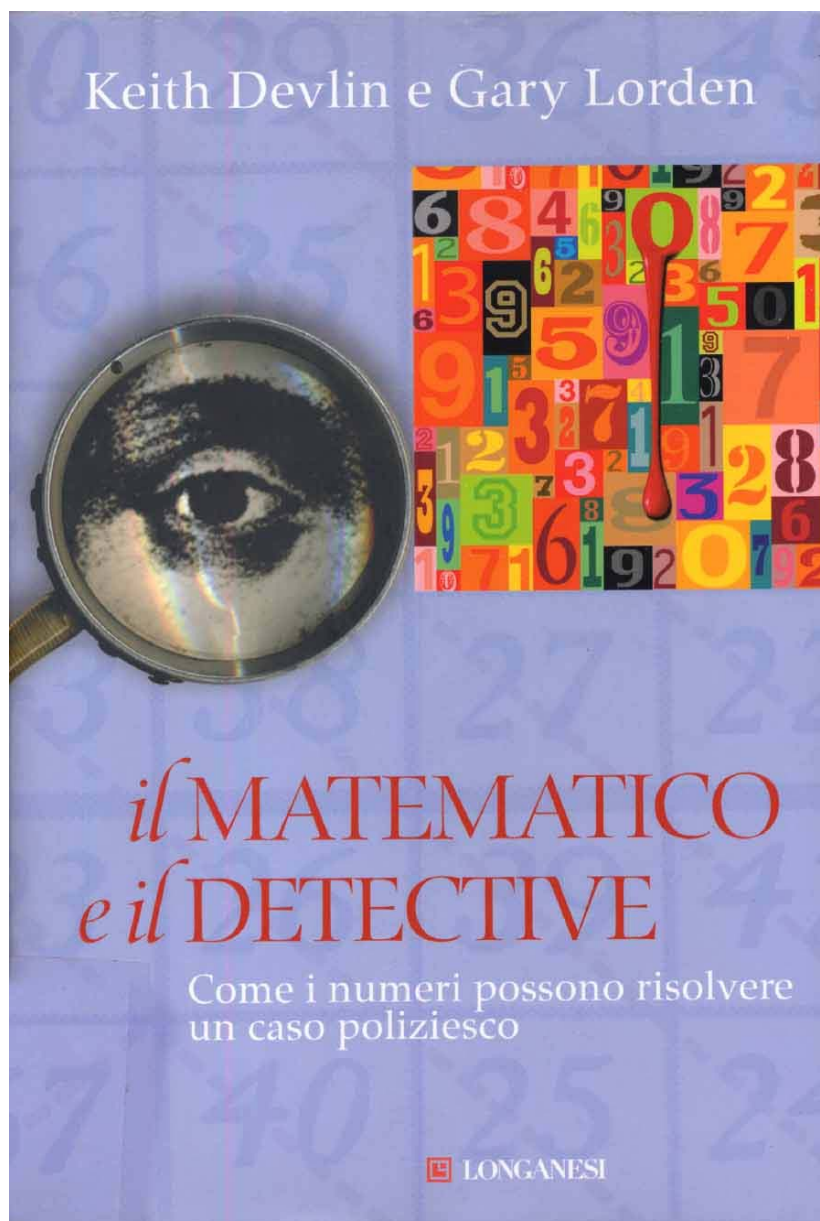
www.longanesi.it ISBN 978-88-304-2495-1

Titolo originale

The Numbers behind NUMB3RS™

Solving Crime with Mathematics

Copyright © 2007 Keith Devlin and Gary Lorden





Indice

IL MATEMATICO E IL DETECTIVE	5
INTRODUZIONE L'EROE È UN MATEMATICO?	5
1 TROVARE LA ZONA CALDA	7
Finzione o realtà?	10
La formula di Rossmo	14
2 COMBATTERE IL CRIMINE CON LA STATISTICA	16
L'angelo della morte	16
La scienza dello Stato	17
Test d'ipotesi	18
Statistica in tribunale?	20
Sorvegliare la polizia	22
Come si accerta l'esistenza di un pregiudizio?	24
3 DATA MINING	26
Brutus	26
Trovare significato nelle informazioni	27
Analisi di legame	28
Raggruppamento genetico	29
Agenti software	33
Apprendimento automatico	34
Reti murali	36
Allenare una rete neurale	38
Estrarre i dati sui crimini con le reti neurali	40
Conosco quella faccia	42
Il caso delle audioconferenze sospette	43
Altri esempi di data mining in NUMB3RS	45
Letture consigliate	45
4 QUANDO È SUCCESSO?	46
Il genio dei numeri nel baseball	46
Individuare i punti di cambiamento	48
Nati nel mondo dell'industria	49
Entra in scena la matematica	50
Scoprire in tempo un attacco bioterroristico	52
5 MIGLIORARE E RICOSTRUIRE LE IMMAGINI	55
Il pestaggio di Reginald Denny	55
Il tatuaggio della rosa	57
Quello che l'occhio non può vedere: la matematica della ricostruzione di immagini	59
Ottimizzazione di immagini: uno sguardo più ravvicinato	61
La matematica in tribunale	62
L'avventura continua...	63
6 PREVEDERE IL FUTURO	66
Caccia all'uomo	66
Prevedere il futuro	67
Come la matematica predisse l'attacco al Pentagono dell'11 settembre	68
Site Profiler	69
Thomas Bayes e le probabilità di ciò che sappiamo	70
Il metodo di Bayes	70
Il caso (fittizio) dell'incidente con omissione di soccorso	71
A caccia dell'assassino evaso	72

7 IL TEST DEL DNA	75
Stati Uniti d’America contro Raymond Jenkins	75
Il profilo genetico	76
Il sistema CODIS dell’FBI	77
Torniamo al caso Jenkins	78
La matematica del profilo genetico	80
Utilizzare il profilo genetico	81
I rischi del colpo a freddo	82
I rapporti NRC le NRC II	83
Numeri in tribunale: le opzioni statistiche	85
Il calcolo della probabilità di una corrispondenza in una banca dati	87
8 SEGRETI: CREARE E DECIFRARE I CODICI	88
L’ipotesi di Riemann	88
www. cybercrime.gov	89
Mantenere i segreti	90
Crittografia a chiave pubblica	92
Firme digitali	97
Che cosa tiene le password al sicuro?	97
9 QUANTO È AFFIDABILE LA PROVA?	101
L’uomo sbagliato?	101
Il mito delle impronte digitali	102
Come vengono «confrontate» le impronte digitali?	104
Gli esperti di impronte digitali si scontrano con i matematici come Charlie Eppes	105
Il caso Brandon Mayfield: un fiasco dell’FBI	107
Che cosa dovrebbe fare un povero matematico?	108
Impronte digitali in rete	109
10 CONNETTERE I PUNTI	112
Una questione in sospeso	112
Un nuovo tipo di guerra, un nuovo tipo di matematica	113
Gli attacchi dell’11 settembre come caso di studio	113
Teoria dei grafi e «misure di centralità»	116
Grafi casuali: strumenti utili per comprendere grandi reti	118
Sei gradi di separazione: «Com’è piccolo il mondo!»	120
Un esempio di connessione dei punti riuscita	121
11 IL DILEMMA DEL PRIGIONIERO, L’ANALISI DEL RISCHIO E IL CONTROTERRORISMO	123
La teoria dei giochi	124
Provaci ancora, Sam	126
Valutazione del rischio	127
La valutazione del rischio come arma contro il terrorismo	128
La ricerca operativa sul contrabbando di armi nucleari	130
Controllare i passeggeri delle linee aeree	136
Due studenti del MIT analizzano il sistema CAPPS	137
12 LA MATEMATICA IN TRIBUNALE	140
La bionda con la coda di cavallo	140
Matematica: evidenza delle prove o magia?	143
Era corretta la conclusione matematica?	144
Il caso del testamento Howland	147
L’uso della matematica nella scelta dei giurati	150
Giurie sotto esame	152
13 REATI AL CASINÒ	154
Sfida a blackjack	154
Il problema del blackjack	155
Contare le carte: un’arma segreta dei matematici	157
La storia di Lorden: prima parte	159
Squadre di giocatori sfidano i casinò	160
Nota a piè di pagina: i matematici e i giochi che scelgono di giocare	162
La storia di Lorden: seconda parte	162

APPENDICE SINOSI MATEMATICA DEGLI EPISODI DELLE PRIME TRE SERIE DI	
NUMB3RS	165
È vera la matematica di NUMB3RS?	165
PRIMA SERIE	167
SECONDA SERIE	171
TERZA SERIE	178
RINGRAZIAMENTI	185
CREDITI DELLE ILLUSTRAZIONI	185

IL MATEMATICO E IL DETECTIVE

INTRODUZIONE L'EROE È UN MATEMATICO?

Il 23 gennaio 2005 una nuova serie televisiva poliziesca intitolata *NUMB3RS* ha debuttato negli Stati Uniti. Creata da Nick Falacci e da sua moglie Cheryl Heuton, la serie è stata prodotta dalla Paramount Network Television e dagli acclamati veterani di Hollywood Ridley e Tony Scott, i cui successi cinematografici comprendono, ad esempio, *Alien*, *Top Gun* e *Il gladiatore*. Per tutta la sua durata, *NUMB3RS* negli Stati Uniti ha regolarmente battuto la concorrenza, affermandosi come la serie televisiva più guardata durante il suo orario il venerdì sera.

Quello che ha sorpreso molti spettatori è che uno dei due eroi dello spettacolo sia un matematico, e che gran parte dell'azione ruoti attorno alla matematica, dal momento che il professor Charlie Eppes impiega le sue potenti capacità per aiutare il fratello maggiore Don, un agente dell'FBI, a identificare e catturare i criminali. Il commento di molti spettatori, e di numerosi critici, è che le storie sono avvincenti, ma la premessa di base è inverosimile: non si può usare la matematica per combattere il crimine, dicono. Ma, come dimostra questo libro, si sbagliano. Si può usare la matematica per risolvere i delitti e le forze di polizia lo fanno davvero, ovviamente non in tutti i casi, ma abbastanza spesso da fare della matematica un'arma potente nella lotta senza fine contro la criminalità. Infatti il primo episodio della serie era fortemente ispirato a un caso vero, come vedremo nel primo capitolo.

Il nostro libro si propone di descrivere, in maniera non tecnica, alcuni dei principali metodi matematici attualmente a disposizione della polizia, della CIA e dell'FBI. La maggior parte di questi metodi sono stati menzionati durante gli episodi di *NUMB3RS*, e anche se spesso collegheremo le nostre spiegazioni a quello che è stato mandato in onda la nostra attenzione sarà focalizzata sulle tecniche matematiche e su come possano essere utilizzate nelle operazioni di polizia. Presenteremo anche alcuni casi veri di crimini risolti con l'ausilio di metodi matematici che non figurano, per lo meno non direttamente, nella serie televisiva.

Per molti aspetti, gli episodi di *NUMB3RS* sono simili a buoni racconti di fantascienza, i quali sono basati su dati fisici e chimici corretti. Ogni settimana *NUMB3RS* presenta una storia inventata in cui tecniche matematiche realistiche svolgono un ruolo cruciale nella narrazione. I produttori di questa serie televisiva fanno tutto il possibile per garantire che i riferimenti matematici utilizzati nei copioni siano corretti e che le applicazioni mostrate siano possibili. Anche se alcuni dei casi presentati sono inventati, sicuramente si tratta di fatti che potrebbero accadere, talvolta senza troppi sforzi di immaginazione. La serie televisiva si concede qualche

licenza poetica, ma questo libro no. Nelle pagine che seguono conoscerete le tecniche matematiche che possono essere utilizzate, e che di fatto vengono utilizzate, per combattere la vera criminalità e per catturare i veri criminali.

TROVARE LA ZONA CALDA

Il profiling geografico dei criminali

L'agente speciale dell'FBI Don Eppes dà un'altra occhiata alla grande mappa stradale di Los Angeles aperta sul tavolo nella sala da pranzo a casa di suo padre. Le croci segnate a penna sulla mappa indicano i luoghi in cui, per diversi mesi, ha colpito uno spietato serial killer, violentando e poi uccidendo un gran numero di giovani donne. Compito di Don è catturare l'assassino prima che colpisca ancora. Ma le indagini sono a un punto di stallo. Don non ha indizi e non sa come procedere.

«Posso aiutarti?» La voce è quella del fratello più giovane di Don, Charlie, brillante professore di matematica al California Institute of Science (CalSci).¹ Don ha sempre ammirato le capacità matematiche di suo fratello, e francamente accoglierebbe volentieri qualunque aiuto egli sia in grado di offrire. Ma... aiuto da un matematico?

«Questo caso non ha a che fare con i numeri, Charlie.» La durezza nella voce di Don è indotta più da frustrazione che da rabbia, ma Charlie sembra non farci caso e la sua risposta, per quanto perentoria, non fa che esprimere un dato di fatto: «*Tutto è numeri*».

Don non è convinto. Naturalmente, ha sentito spesso Charlie dire che tutta la matematica ha a che fare con schemi: con la loro identificazione, con l'analisi e l'elaborazione di previsioni su di essi. Ma non occorre un genio della matematica per vedere che le croci sulla mappa sono distribuite in modo totalmente casuale. Non c'è alcuno schema, nessun modo per prevedere dove andrà messa la prossima croce, il luogo preciso in cui verrà aggredita la prossima ragazza. Potrebbe anche succedere proprio stasera. Se solo ci fosse qualche regolarità nella disposizione delle croci, uno schema che possa essere catturato da un'equazione matematica, nel modo in cui, come Don ricorda dai giorni di scuola, l'equazione $x^2 + y^2 = 9$ descrive un cerchio...

Guardando la mappa, persino Charlie deve ammettere che non c'è modo di usare la matematica per prevedere dove l'assassino colpirà la prossima volta. Vaga per la stanza fino alla finestra e si ferma a fissare il giardino, mentre il silenzio della sera è interrotto soltanto dal *continuo flic flic flic flic* dell'irrigatore automatico che annaffia il prato. Gli occhi di Charlie vedono l'irrigatore ma la sua mente è lontana. Deve ammettere che Don ha probabilmente ragione. La matematica può essere usata per tantissime cose, molte più di quelle che la maggior parte della gente può immaginare. Ma perché la matematica possa entrare in gioco deve esistere una sorta di schema.

Flic flic flic flic. L'irrigatore continua a fare il suo lavoro. C'è quel brillante matematico di New York che ha usato la matematica per studiare come funziona il cuore, aiutando i medici a individuare minime irregolarità nel battito cardiaco prima

¹ Il California Institute of Science (CalSci) è un'università fittizia, chiaramente ispirata al reale California Institute of Technology (Caltech) di Pasadena in cui sono girate alcune scene del telefilm. (*N.d. T.*)

che una persona sia colpita da un infarto.

Flic flic flic flic. Ci sono i programmi informatici basati sulla matematica che le banche utilizzano per seguire l'andamento degli acquisti con le carte di credito, in cerca di un brusco cambiamento nello schema che potrebbe indicare un furto di identità o una carta rubata.

Flic flic flic flic. Senza ingegnosi algoritmi matematici, il telefono cellulare nella tasca di Charlie sarebbe grande il doppio e molto più pesante.

Flic flic flic flic. A ben vedere, è difficile pensare a un'area della vita moderna che non dipenda, spesso in modo cruciale, dalla matematica. Ma deve esserci uno schema, o l'analisi matematica non può neppure incominciare.

Flic flic flic flic. Per la prima volta Charlie nota l'irrigatore, e improvvisamente ha un'idea: ecco la risposta! Ora Charlie può aiutare Don a risolvere il caso e la soluzione è sempre stata lì, davanti ai suoi occhi. Semplicemente non se ne era accorto.

Trascina Don vicino alla finestra. «Ci stavamo ponendo la domanda sbagliata», afferma. «In base a quello che sai, non c'è modo di prevedere dove l'assassino colpirà la prossima volta.» Indica l'irrigatore col dito. «Proprio come, anche se studiassimo tutti i punti in cui ogni goccia d'acqua cade sull'erba, non potremmo comunque prevedere dove cadrà la prossima goccia. C'è troppa incertezza.» Lancia un'occhiata a Don per assicurarsi che stia ascoltando. «Ma supponiamo che tu non possa vedere l'irrigatore, e che tu conosca soltanto la distribuzione dei punti in cui sono cadute le gocce d'acqua. Allora, usando la matematica, potresti calcolare il luogo esatto in cui deve trovarsi l'irrigatore. Non puoi usare lo schema delle gocce per prevedere dove cadrà la prossima goccia, ma puoi usarlo per risalire alla fonte. Vale lo stesso per il tuo assassino.»

Don trova difficile accettare quello che suo fratello sembra suggerire. «Charlie, mi stai dicendo che sei in grado di capire dove vive l'assassino?»

La risposta di Charlie è semplice: «Sì».

Don non è ancora del tutto convinto che l'idea di Charlie possa funzionare, ma è colpito dalla sicurezza e dal fervore di suo fratello, e così gli permette di aiutarlo nelle indagini.

Il primo passo per Charlie è imparare alcuni fondamenti di criminologia: per prima cosa, come si comportano i serial killer? La sua esperienza di matematico gli ha insegnato come riconoscere i fattori cruciali e ignorare tutti gli altri, in modo che un problema apparentemente complesso possa essere ridotto a uno più semplice, con un numero limitato di variabili chiave. Parlando con Don e con gli altri agenti all'ufficio dell'FBI in cui lavora suo fratello, Charlie apprende, ad esempio, che i criminali seriali violenti esibiscono certe tendenze nella scelta dei luoghi dei delitti. Tendono a colpire vicino a casa, ma non troppo vicino; delineano sempre una «zona cuscinetto» attorno alla propria residenza che escluderanno dal loro raggio d'azione: un'area troppo vicina per potersi sentire al sicuro; fuori da quella zona di sicurezza, la frequenza dei luoghi dei delitti diminuisce all'aumentare della distanza da casa.

Tornato nel suo ufficio al dipartimento di matematica del CalSci, Charlie inizia a lavorare sodo, riempiendo freneticamente le lavagne di equazioni e formule matematiche. Obiettivo: trovare la chiave matematica per determinare una «zona

calda»: un'area sulla mappa, desunta dai luoghi dei delitti, in cui è più probabile che viva l'assassino.

Come succede ogni volta che Charlie lavora a un difficile problema di matematica, le ore volano tra un tentativo fallito e un altro. Poi, finalmente, ha un'idea che pensa dovrebbe funzionare. Cancella ancora una volta i suoi scarabocchi e scrive sulla lavagna questa formula dall'aspetto complicato:²

$$p_{ij} = k \sum_{n=1}^c \left[\frac{\varphi}{\left(|x_i - x_n| + |y_j - y_n| \right)^f} + \frac{(1 - \varphi)(B^{g-f})}{\left(2B - |x_i - x_n| - |y_j - y_n| \right)^g} \right]$$

«Questa dovrebbe funzionare», dice a se stesso.

Il prossimo passo è mettere a punto la formula controllando se funziona in relazione agli esempi di crimini passati che Don gli fornisce. Immettendo nella formula i luoghi dei delitti relativi ai casi precedenti, si riesce a prevedere esattamente dove vivevano i criminali? Questo è il momento della verità, in cui Charlie si renderà conto se i suoi calcoli riflettano o meno la realtà. Talvolta non è così, e in effetti Charlie capisce che nella scelta iniziale dei fattori da tenere in considerazione deve aver sbagliato qualcosa. Ma dopo qualche piccolo ritocco la formula sembra funzionare.

Il giorno dopo, traboccante di energia e sicurezza, Charlie si presenta negli uffici dell'FBI portando una stampata della mappa indicante i luoghi dei delitti con la «zona calda» ben evidenziata. Proprio come l'equazione $x^2 + y^2 = 9$ descrive un cerchio, in modo che quando viene inserita in un computer adeguatamente programmato esso disegna un cerchio, analogamente, quando Charlie ha immesso la sua nuova equazione nel computer, anch'esso ha prodotto una figura. Questa volta non un cerchio; l'equazione di Charlie è molto più complessa. Ciò che il computer ha generato è una serie di regioni concentriche colorate sulla mappa di Los Angeles situate sulla zona calda in cui vive l'assassino.

Questa mappa non pone certo fine al lavoro di Don e dei suoi colleghi, ma trovare l'assassino non è più come cercare un ago in un pagliaio. Grazie alla matematica di Charlie, il pagliaio si è improvvisamente ridotto a niente più che una balla di fieno.



Charlie spiega a Don e agli altri agenti dell'FBI impegnati nel caso che il criminale ha cercato di nascondere dove vive, scegliendo le vittime in quello che considerava

² Analizzeremo meglio questa formula più avanti.

uno spettro casuale di luoghi, ma che, malgrado i suoi tentativi, la formula matematica rivela la verità: una zona calda in cui è localizzata la residenza del criminale con una probabilità molto alta. Don e la sua squadra decidono di indagare sugli uomini di una certa fascia di età che vivono nella zona calda, e di piantonarli di nascosto in modo da ottenere prove di DNA dai mozziconi di sigarette, dalle cannuce e da cose simili abbandonate dai sospetti, che potrebbero corrispondere al DNA trovato sulle scene dei delitti.

Dopo qualche giorno - e qualche momento di alta tensione - catturano il loro uomo. Il caso è risolto. Don dice al fratello più giovane: «Hai trovato *una gran bella formula*, Charlie».

Finzione o realtà?

Tralasciando qualche spettacolare colpo di scena, quello che abbiamo descritto sopra è ciò che il pubblico televisivo ha visto nel primissimo episodio di *NUMB3RS* trasmesso per la prima volta negli Stati Uniti il 23 gennaio 2005. Molti spettatori non riuscivano a credere che la matematica potesse servire a catturare un criminale in questo modo. In realtà, il primo episodio era interamente basato, in maniera piuttosto fedele, su un caso vero nel quale era stata usata un'unica equazione matematica per identificare la zona calda in cui viveva il criminale. Era la stessa equazione, riprodotta sopra, che gli spettatori hanno visto scrivere da Charlie sulla sua lavagna.

Il matematico che nella vita reale creò la formula si chiama Kim Rossmo. La tecnica che utilizza la matematica per dedurre il luogo in cui potrebbe abitare un criminale seriale, che Rossmo aiutò a mettere a punto, è chiamata *profiling geografico*.

Negli anni '80 del Novecento Rossmo era un giovane agente della polizia a Vancouver, in Canada. Ciò che era insolito per un agente di polizia era il suo talento per la matematica. Per tutti gli anni di scuola era stato un «piccolo genio della matematica», il genere di studente che innervosisce un po' i compagni, e spesso anche gli insegnanti. Si racconta che durante l'ultimo anno della scuola superiore, annoiato dalla lentezza con cui procedeva il suo corso di matematica, abbia chiesto di sostenere l'esame finale nella seconda settimana del semestre. Dopo aver ottenuto un punteggio del cento per cento, fu esonerato dal resto del corso.

Ugualmente annoiato dal tipico avanzamento lento delle indagini di polizia sui serial killer, Rossmo decise di tornare a studiare, e fu così che divenne il primo poliziotto canadese a conseguire un dottorato di ricerca in criminologia presso la Simon Fraser University. I supervisori della sua tesi, Paul e Patricia Brantingham, erano stati dei pionieri dell'applicazione di modelli matematici (essenzialmente insiemi di equazioni che descrivono una situazione) al comportamento criminale, studiando in particolare i modelli che descrivono dove è più probabile che i crimini avvengano in base a dove un criminale vive, lavora e si muove abitualmente. (Erano stati i Brantingham a notare gli schemi di distribuzione dei luoghi nei casi di crimini che Don e i suoi colleghi illustrano a Charlie nel corso della puntata televisiva di *NUMB3RS*.)

L'interesse di Rossmo era un po' diverso da quello dei Brantingham. In qualità di agente di polizia, Rossmo non intendeva studiare i modelli del comportamento criminale, bensì utilizzare i dati effettivi sui luoghi dei reati collegati a un singolo delinquente sconosciuto come *strumento investigativo* per aiutare la polizia a scovare il criminale.

Rossmo riscosse qualche successo iniziale nel riesame di vecchi casi, e dopo aver terminato il dottorato di ricerca ed essere stato promosso al rango di ispettore investigativo coltivò il proprio interesse mettendo a punto migliori metodi matematici per effettuare quello che chiamò il *targeting* geografico dei criminali (CGT, *Criminal Geographic Targeting*). Altri definirono il metodo «*profiling* geografico»; in quanto faceva da complemento alla ben nota tecnica di «*profiling* psicologico» impiegata dagli investigatori per trovare i criminali sulla base delle loro motivazioni e caratteristiche psicologiche. Il *profiling* geografico tenta di localizzare una probabile base operativa per un criminale analizzando i luoghi dei suoi reati.

Rossmo concepì l'idea al cuore della sua formula apparentemente magica mentre si trovava su un treno ad alta velocità in Giappone, un giorno del 1991. Non avendo un taccuino su cui scrivere, la abbozzò su un tovagliolo di carta. Con qualche ritocco successivo, la formula divenne l'elemento principale di un programma informatico elaborato da Rossmo, chiamato Rigel (dall'omonima stella nella costellazione di Orione, il Cacciatore). Oggi Rossmo vende Rigel, assieme a servizi di preparazione e consulenza, alla polizia e ad altre agenzie di investigazioni in tutto il mondo per aiutarle a trovare i criminali.

Quando Rossmo descrive come funziona Rigel alle forze di polizia interessate al programma, cita la sua metafora preferita: quella di determinare la collocazione di un irrigatore rotante da giardino analizzando lo schema delle gocce d'acqua che spruzza sul terreno. Mentre lavoravano al loro episodio pilota i creatori di *NUMB3RS*, Cheryl Heuton e Nick Falacci, hanno preso in prestito la metafora di Rossmo per descrivere il modo in cui Charlie concepisce la formula e spiega l'idea al fratello.

Rossmo ebbe qualche successo con le indagini sui criminali seriali in Canada, ma ciò che davvero lo rese molto famoso tra i distretti di polizia di tutto il Nordamerica fu il caso dello stupratore di Lafayette, in Louisiana, noto con il nome di *South Side Rapist* (lo stupratore della zona sud).

Per più di dieci anni un aggressore sconosciuto, con la faccia avvolta da una sciarpa come un bandito, aveva molestato e assalito molte donne nella città. Nel 1998 la polizia locale, sommersa da migliaia di segnalazioni e un uguale numero di sospetti, chiese aiuto a Rossmo. Utilizzando Rigel, Rossmo analizzò i dati relativi ai luoghi dei reati e realizzò una mappa molto simile a quella mostrata da Charlie in *NUMB3RS*, con bande di colore indicanti la zona calda e i suoi anelli interni sempre più caldi man mano che ci si avvicina al centro. La mappa permise alla polizia di limitare le indagini a un'area poco estesa, pari a poco più di un chilometro quadrato, e a circa una dozzina di sospetti. Alcuni agenti in incognito rastrellarono la zona calda impiegando le stesse tecniche rappresentate in *NUMB3RS*, per ottenere campioni di DNA di tutti i maschi della fascia d'età sospetta abitanti nella zona.

Ci fu un momento di frustrazione quando tutti i sospetti nella zona calda furono scagionati dai test del DNA. Ma poi intervenne un colpo di fortuna. L'investigatore

capo McCullan «Mac» Gallien ricevette una segnalazione anonima che indicava un sospetto molto improbabile: un vicesceriffo di un distretto vicino. Trattandosi solo dell'ennesima goccia nel mare delle segnalazioni che aveva già raccolto, Mac era tentato di archivarla senza farci caso, ma poi, per scrupolo, decise di controllare l'indirizzo del sospetto. Non era nemmeno vicino alla zona calda. Ma poiché qualcosa continuava a turbarlo, decise di indagare un po' più a fondo. E alla fine fece centro: il vicesceriffo aveva cambiato casa e la sua precedente abitazione si trovava proprio nella zona calda! Il reperto di DNA fu raccolto da un mozzicone di sigaretta e si rivelò corrispondente a quello prelevato nei luoghi dei delitti. Il vicesceriffo fu arrestato e Rossmo divenne subito una celebrità nel mondo della lotta contro il crimine.

Curiosamente, mentre scrivevano l'episodio pilota di *NUMB3RS*, basato su questo caso vero, Heuton e Falacci non hanno potuto fare a meno di incorporare il medesimo colpo di scena nel finale. Quando Charlie applica per la prima volta la sua formula, non viene trovata alcuna corrispondenza tra il DNA dei sospetti abitanti nella zona calda e i campioni prelevati dai luoghi dei delitti, proprio come accadde con la formula di Rossmo a Lafayette. La fede di Charlie nella sua analisi matematica è così forte che quando Don gli dice che la ricerca è fallita, all'inizio si rifiuta di accettare questo risultato. «Dovete averlo mancato», dice.

Frustrato e deluso, Charlie si consulta con Don a casa del loro padre Alan, e Alan dice: «Sono certo che il problema non è la matematica, Charlie. Deve essere qualcos'altro». Queste parole fanno capire a Don che trovare la *residenza* dell'assassino potrebbe essere l'obiettivo sbagliato. «Se tu cercassi di trovarmi nel luogo in cui *vivo*, probabilmente falliresti perché non sono lì quasi mai», osserva. «Di solito sono *al lavoro*.» Charlie accoglie questa idea per seguire una differente linea di attacco, modificando i suoi calcoli in modo da cercare *due* zone calde: una che potrebbe contenere l'abitazione del killer e l'altra il suo posto di lavoro. Questa volta la matematica di Charlie funziona, e Don riesce a identificare e a catturare il criminale poco prima che uccida un'altra vittima.

Oggigiorno, la società di Rossmo ECRI (Environmental Criminology Research, Inc.) offre il pacchetto informatico brevettato Rigel insieme a un servizio che insegna come utilizzarlo efficacemente per risolvere i crimini. Rossmo *stesso* viaggia per il mondo, in Asia, Africa, Europa e Medio Oriente per offrire il suo aiuto nelle indagini e dare lezioni a poliziotti e criminologi. Occorrono due anni di addestramento, impartito da Rossmo o da uno dei suoi assistenti, per imparare ad adattare l'uso del programma alle caratteristiche specifiche di un particolare comportamento criminale.

Rigel non è sempre garanzia di successo. Nell'ottobre del 2002, in un caso che divenne noto con il nome di *Beltway Sniper Case* (il caso del cecchino della circonvallazione), nel giro di tre settimane dieci persone furono uccise e altre tre gravemente ferite da quella che si scoprì essere una coppia di serial killer operante all'interno e nelle vicinanze dell'area di Washington, DC. Quando Rossmo fu chiamato in aiuto, concluse che la base del cecchino doveva trovarsi da qualche parte nei sobborghi a nord di Washington, ma in seguito si scoprì che i due assassini non vivevano in quell'area e si spostavano troppo spesso per poter essere localizzati dal *profiling* geografico.

Il fatto che Rigel non funzioni sempre non sarà una sorpresa per chiunque abbia familiarità con ciò che accade quando si cerca di applicare la matematica al caotico mondo reale delle persone. Molti escono dalla loro esperienza alle scuole superiori convinti che esista un modo giusto e uno sbagliato di usare la matematica per risolvere i problemi: per lo più quello dell'insegnante è il modo giusto e i loro tentativi sono il modo sbagliato. Ma raramente le cose stanno in questo modo. La matematica darà sempre la risposta giusta (se usata correttamente) quando la si applica a situazioni fisiche molto ben definite, come calcolare la quantità di carburante di cui un jet ha bisogno per volare da Los Angeles a New York. (Vale a dire, la matematica fornirà la risposta corretta ammesso che si parta da dati precisi sul peso totale dell'aeroplano, dei passeggeri e del carico, sui venti prevalenti, e così via. Se si omette di incorporare qualche dato fondamentale nelle equazioni matematiche quasi sempre si perverrà a una risposta imprecisa.) Ma quando la matematica viene applicata a un problema sociale, come un crimine, raramente le cose sono così chiare.

Quando si elaborano equazioni capaci di cogliere elementi di qualche attività della vita reale si dice che viene costruito un «modello matematico». Nel costruire un modello *fisico* di qualcosa, poniamo un aeroplano da studiare in una galleria del vento, la cosa importante è riprodurre tutto nel modo giusto, a parte le dimensioni e i materiali usati. Nel costruire un modello matematico, l'idea è di riprodurre nel modo giusto il *comportamento* che ci interessa. Ad esempio, per essere utile, un modello matematico del clima dovrebbe prevedere pioggia per i giorni in cui piove e sole per i giorni in cui il cielo è sereno. La cosa più difficile di solito è proprio costruire il modello. «Eseguire i calcoli matematici» del modello - vale a dire, risolvere le equazioni che lo costituiscono - è generalmente molto più semplice, soprattutto quando si usano i computer. I modelli matematici delle condizioni meteorologiche spesso non funzionano perché il clima è un fenomeno troppo complicato (nel linguaggio di tutti i giorni, è «troppo imprevedibile») per poter essere catturato dalla matematica con un alto grado di accuratezza.

Come vedremo più avanti, di solito non esiste una cosa come «un modo corretto» di usare la matematica per risolvere i problemi nel mondo reale, in particolare quelli che coinvolgono le persone. Per cercare di affrontare le sfide con cui Charlie deve fare i conti in *NUMB3RS* - localizzare i criminali, studiare la diffusione di una malattia o la circolazione di denaro falso, prevedere la scelta dei bersagli dei terroristi, e così via - un matematico non può limitarsi a scrivere un'equazione e a risolverla. Ci vuole una certa abilità a mettere insieme una grande quantità di informazioni e di dati, selezionare le variabili matematiche che descrivono una situazione e poi creare un modello della suddetta situazione mediante un insieme di equazioni. E una volta costruito un modello, resta ancora il problema di risolverlo in qualche modo, attraverso approssimazioni, calcoli o simulazioni al computer. Ogni passo nel processo richiede buonsenso e creatività. Due matematici che lavorano in maniera indipendente, per quanto brillanti, non produrranno mai risultati identici, ammesso che siano in grado in generale di pervenire a qualche risultato utile.

Non sorprende affatto, allora, che nel campo *del profiling* geografico Rossmo abbia qualche concorrente. Grover M. Godwin del Justice Center dell'Università dell'Alaska, autore del libro *Hunting Serial Predators*, ha messo a punto un pacchetto

informatico chiamato Predator che usa una branca della statistica matematica nota con il nome di analisi multivariata per localizzare l'abitazione di un serial killer analizzando i luoghi dei reati, i posti in cui le vittime sono state viste l'ultima volta, e quelli in cui sono stati ritrovati i cadaveri. Ned Levine, un pianificatore urbanistico di Houston, ha messo a punto un programma chiamato Crimestat per il National Institute of Justice, una succursale di ricerca del dipartimento della Giustizia degli Stati Uniti. Esso utilizza un ramo della statistica chiamato «statistica spaziale» per analizzare i dati relativi ai criminali seriali, e può anche essere impiegato per aiutare gli agenti a comprendere fenomeni come la distribuzione degli incidenti automobilistici o la diffusione delle malattie. David Canter, professore di psicologia all'Università di Liverpool in Inghilterra, dove è anche direttore del Centre for Investigative Psychology, ha messo a punto il proprio programma informatico, Dragnet, che qualche volta ha offerto gratis ai ricercatori. Canter ha fatto notare che finora nessuno ha effettuato un confronto serrato dei vari sistemi informatico-matematici per localizzare i criminali seriali applicandoli agli stessi casi, e in alcune interviste ha affermato che sul lungo termine il suo programma e altri si riveleranno accurati almeno quanto Rigel.

La formula di Rossmo

Per finire, vediamo più da vicino la formula che Rossmo scribacchiò sul tovagliolo di carta mentre si trovava sul treno ad alta velocità in Giappone nel 1991.

$$p_{ij} = k \sum_{n=1}^c \left[\frac{\varphi}{(|x_i - x_n| + |y_j - y_n|)^f} + \frac{(1 - \varphi)(B^{g-f})}{(2B - |x_i - x_n| - |y_j - y_n|)^g} \right]$$

Per capire che cosa significa, si immagini di sovrapporre alla mappa una rete formata da tanti piccoli quadrati, ognuno contrassegnato da due numeri, «i» e «j», indicanti rispettivamente la riga e la colonna in cui si trova. La probabilità, p_{ij} , che la residenza dell'assassino sia in quel quadrato è scritta nel primo membro dell'equazione, e il secondo membro mostra come calcolarla. I luoghi dei reati sono rappresentati attraverso coordinate cartografiche, (x_1, y_1) per il primo crimine, (x_2, y_2) per il secondo e così via. Ciò che la formula dice è questo:

Per ottenere la probabilità p_{ij} per il quadrato posto nella riga «i» e nella colonna «j» della rete, prima si deve calcolare la distanza che occorre coprire per andare dal punto centrale (x_i, y_i) di quel quadrato a ciascun luogo del reato (x_n, y_n) .

La lettera «n» indica qualunque luogo del reato: $n=1$ vuol dire «primo crimine», $n=2$ «secondo crimine», e così via. La risposta alla domanda «che distanza occorre coprire?» è:

$$|x_i - x_n| + |y_j - y_n|$$

e questa si usa in due modi.

Leggendo la formula da sinistra a destra, il primo modo è mettere quella distanza al

denominatore e ϕ al numeratore. La distanza è elevata alla potenza f . La scelta del valore di f dipenderà da quale funziona meglio quando la formula viene messa alla prova immettendo dati relativi a casi di crimini passati. (Se prendiamo $f=2$, ad esempio, quella parte della formula assomiglierà alla «legge dell'inverso del quadrato» che descrive la forza di gravità.) Questa parte della formula esprime l'idea che, una volta usciti dalla zona cuscinetto, la probabilità di trovare luoghi del reato *diminuisce* all'aumentare della distanza.

Il secondo modo in cui la formula utilizza la «distanza di viaggio» associata a ciascun crimine coinvolge la zona cuscinetto. Nella seconda frazione, si *sottrae* la distanza da $2B$, dove B è un numero che sarà scelto per descrivere le dimensioni della zona cuscinetto. La sottrazione produce *risultati più piccoli* man mano che la distanza aumenta, di modo che elevando quei risultati a un'altra potenza, g , nel denominatore della seconda parte della formula, si ottengono *valori più grandi*.

Insieme, la prima e la seconda parte della formula svolgono una sorta di «azione di equilibrio», esprimendo il fatto che quando ci si allontana dall'abitazione del criminale la probabilità dei reati prima *aumenta* (nell'ambito della zona cuscinetto) e poi *diminuisce*. Le due parti della formula sono combinate utilizzando uno strano segno matematico, la lettera greca Σ , che sta per «sommare (addizionare) i contributi da ciascuno dei crimini alla valutazione della probabilità per il quadrato della rete 'ij'». La lettera greca ϕ è usata nelle due parti come un modo per dare più «peso» a una parte o all'altra. La scelta di un valore più grande di ϕ dà maggior peso al fenomeno per cui «la probabilità diminuisce man mano che la distanza aumenta», mentre un valore di ϕ più piccolo enfatizza l'effetto della zona cuscinetto.

Una volta calcolate le probabilità, p_{ij} , di tutti i quadratini della rete, è facile creare una mappa della zona calda. Basta colorare i quadrati utilizzando, ad esempio, giallo acceso per le probabilità più alte, arancione per quelle un po' più basse, poi rosso e così via, lasciando non colorati i quadrati con bassa probabilità.

La formula di Rossmo è un buon esempio dell'arte di usare la matematica per descrivere una conoscenza incompleta dei fenomeni del mondo reale. Diversamente dalla legge di gravità, che attraverso misurazioni attente può essere vista operare *tutte le volte allo stesso modo*, le descrizioni del comportamento di singoli esseri umani sono nella migliore delle ipotesi approssimative e incerte. Quando Rossmo verificò la sua formula su crimini passati, dovette trovare la forma che meglio si adattava ai dati scegliendo diversi valori possibili di f e g , così come di B e ϕ . Utilizzò poi quei risultati per analizzare gli schemi di crimini successivi, lasciando aperto lo spazio per ulteriori aggiustamenti in ogni nuova investigazione.

Il metodo di Rossmo non è certamente paragonabile a una scienza precisa come quella impiegata per costruire i missili: il viaggio nello spazio dipende in modo cruciale dal fatto di ottenere sempre la risposta giusta con un alto grado di accuratezza. Ma è comunque scienza. Non funziona in tutti i casi e le risposte che fornisce sono solo probabilità. In criminologia e altri ambiti che coinvolgono il comportamento umano, però, conoscere queste probabilità può fare una notevole differenza.

COMBATTERE IL CRIMINE CON LA STATISTICA

L'angelo della morte

Nel 1996 Kristen Gilbert, trentatreenne, divorziata, madre di due figli di sette e dieci anni e infermiera nel reparto C del Veteran's Affairs Medical Center di Northampton, nel Massachusetts, si era fatta una certa reputazione tra i suoi colleghi d'ospedale. In diverse occasioni era stata la prima a notare che un paziente stava per avere un arresto cardiaco e a suonare un «codice blu» per chiamare la squadra di rianimazione. Rimaneva sempre calma, ed era competente ed efficiente nel seguire il paziente. Talvolta aveva cercato di riattivare il battito cardiaco dei pazienti, prima dell'arrivo della squadra d'emergenza, con un'iniezione di epinefrina, un cardiostimolante, e così a volte aveva loro salvato la vita. I colleghi le avevano dato il soprannome di «angelo della morte».

Ma quello stesso anno tre infermieri si rivolsero alle autorità per esprimere i loro crescenti sospetti che la faccenda non fosse del tutto chiara. A loro avviso, si erano verificati troppi decessi per arresto cardiaco in quel particolare reparto. Erano state rilevate anche molte inspiegabili diminuzioni delle scorte di epinefrina. Gli infermieri iniziavano a temere che Kristen Gilbert somministrasse ai pazienti forti dosi del farmaco per indurre gli stessi attacchi cardiaci, in modo da poter poi recitare la parte dell'eroina che cercava di salvarli. Il soprannome «angelo della morte» cominciava a suonare ancor più azzeccato di come lo avevano concepito inizialmente.

L'ospedale avviò un'indagine, ma non trovò nulla di irregolare. In particolare, a quanto dissero, il numero di morti per arresto cardiaco in quella unità era più o meno in linea con le frequenze osservate in altri ospedali VA (Veteran's Affairs). Nonostante i risultati delle indagini iniziali, tuttavia, il personale dell'ospedale continuò a nutrire dei sospetti e alla fine fu avviata una seconda indagine. Questa volta fu chiamato un esperto studioso di statistica, Stephen Gehlbach dell'Università del Massachusetts, affinché esaminasse meglio le cifre relative agli arresti cardiaci e ai decessi in quella unità. In gran parte come conseguenza dell'analisi di Gehlbach, nel 1998 l'US Attorney's Office decise di riunire un gran giuri per sentire le prove contro Kristen Gilbert.

Parte del corpo di prove era il suo presunto movente. Oltre alla ricerca dell'esperienza eccitante di lanciare l'allarme «codice blu» e di assistere al processo di rianimazione, nonché dei riconoscimenti per aver lottato valorosamente tentando di salvare il paziente, alcuni suggerivano che a motivare le sue azioni fosse anche il desiderio di fare colpo sul fidanzato, che lavorava nello stesso ospedale. Per di più, l'imputata aveva accesso all'epinefrina. Ma siccome nessuno in realtà l'aveva mai vista fare una di queste presunte iniezioni letali, le accuse contro di lei, per quanto

suggestive, erano puramente circostanziali. Anche se i pazienti interessati erano per lo più uomini di mezza età che non erano considerati potenziali vittime di un attacco cardiaco, non era comunque escluso che i loro infarti si fossero verificati naturalmente. Ciò che fece pendere la bilancia dalla parte dell'accusa, e portò alla decisione di incriminare Kristen Gilbert per pluriomicidio, fu l'analisi statistica di Gehlbach.

La scienza dello Stato

La statistica è largamente usata dalla polizia in molti modi e per svariati scopi. In *NUMB3RS*, Charlie compie spesso un'analisi statistica, e l'impiego di tecniche statistiche apparirà in molti capitoli di questo libro, spesso senza un nostro riferimento esplicito. Ma che cos'è esattamente la statistica?

Il termine inglese *statistics* è apparentato all'espressione latina *statisticum collegium*, che significa «consiglio di Stato». La parola italiana *statista* riflette gli usi iniziali della tecnica. Analogamente, la parola tedesca *Statistik* significava in origine l'analisi dei dati relativi allo Stato. Fino al XIX secolo il termine inglese equivalente era *political arithmetic* (aritmetica politica), in seguito al quale fu introdotta la parola *statistics* per fare riferimento a qualunque collezione o classificazione di dati.

Oggi, *statistics* ha effettivamente due significati collegati tra loro. Il primo è la collezione e tabulazione dei dati; il secondo è l'uso di strumenti matematici e di altri metodi per trarre conclusioni significative e utili dai dati catalogati. Alcuni studiosi di statistica chiamano la prima attività *little-s statistics* (statistica con la s minuscola) e la seconda *big-S Statistics* (Statistica con la S maiuscola). Intesa con la s minuscola, la parola *statistics* nella lingua inglese è trattata al plurale quando si riferisce a una collezione di numeri. Ma è singolare quando è usata per indicare l'attività di collezione e sistemazione di tali numeri. *Statistics* (con la S maiuscola) si riferisce a un'attività ed è pertanto singolare.

Sebbene molti tifosi sportivi e altre categorie di persone si divertano a collezionare e a tabulare dati numerici, il vero valore della statistica con la s minuscola è quello di fornire i dati per la Statistica con la S maiuscola. Molte delle tecniche impiegate nella Statistica con la S maiuscola coinvolgono la branca della matematica nota come teoria della probabilità, il cui studio ebbe inizio nel XVI e nel XVII secolo come tentativo di comprendere i probabili risultati dei giochi d'azzardo, in modo da accrescere le probabilità di vittoria. Ma mentre la teoria della probabilità è una branca specifica della matematica, la Statistica è essenzialmente una scienza applicata che usa metodi matematici.

Per quanto i servizi di polizia collezionino una grande quantità di statistiche (con la s minuscola), noi ci concentreremo sull'uso della Statistica con la S maiuscola come strumento nella lotta contro il crimine. (Da questo momento in poi abbandoneremo la terminologia «S maiuscola», «s minuscola» e utilizzeremo la parola «statistica» nel modo in cui fanno gli statistici, ovvero per indicare entrambi i significati, lasciando al lettore il compito di stabilire a quale ci si riferisce in base al contesto.)

Sebbene alcune applicazioni della statistica nelle indagini di polizia facciano uso di metodi sofisticati, le tecniche di base insegnate in un corso universitario di statistica del primo anno sono spesso sufficienti per risolvere un caso.

Questo fu sicuramente vero per il caso *Stati Uniti contro Kristen Gilbert*. Una domanda cruciale per il gran giurì era se il numero di decessi nell'unità ospedaliera quando Kristen Gilbert era in servizio era significativamente maggiore rispetto ad altri periodi. La parola chiave qui è «significativamente». Una o due morti in più nel suo orario di lavoro potevano essere una coincidenza. Quante morti servivano per raggiungere il livello di «significatività» sufficiente a fondare le accuse contro Kristen Gilbert? Questa è una domanda cui solo la statistica è in grado di rispondere. È così che Stephen Gehlbach fu chiamato a presentare al gran giurì un sunto delle sue scoperte.

Test d'ipotesi

La deposizione di Gehlbach era basata su una fondamentale tecnica statistica nota come test d'ipotesi. Tale metodo utilizza la teoria della probabilità per stabilire se un risultato sia o meno così insolito da rendere altamente improbabile che si sia verificato naturalmente.

Una delle prime cose che fece Gehlbach fu riportare in un grafico i numeri annuali di decessi all'ospedale dal 1988 al 1997, suddivisi per turni: da mezzanotte alle 8.00, dalle 8.00 alle 16.00 e dalle 16.00 a mezzanotte. Il grafico risultante è mostrato nella figura 1. Ogni barra verticale mostra il numero totale di decessi nell'anno durante quel turno particolare.

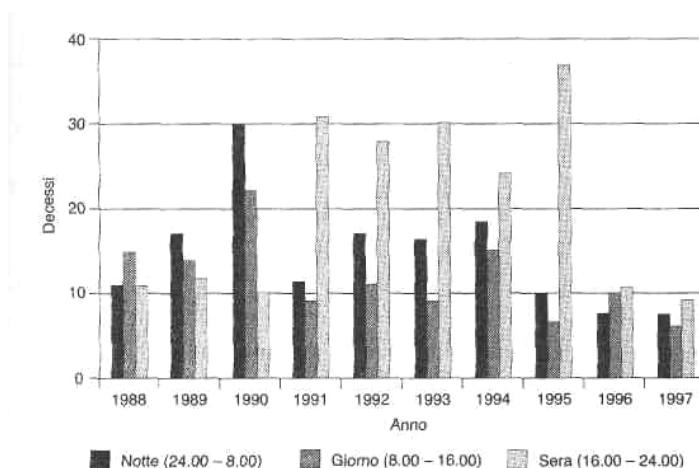


Figura 1. Numero totale di decessi nell'ospedale, suddivisi per turno e anno.

Il grafico mostra un andamento preciso. Per i primi due anni, abbiamo circa dieci decessi l'anno durante ciascun turno. Poi, per tutti gli anni compresi tra il 1990 e il 1995, uno dei tre turni mostra tra venticinque e trentacinque decessi l'anno. Infine, negli ultimi due anni, si ritorna a circa dieci decessi in ciascuno dei tre turni. Quando gli investigatori esaminarono il curriculum professionale di Kristen Gilbert,

scoprirono che era entrata a far parte del personale del reparto C nel marzo del 1990 e aveva smesso di lavorare all'ospedale nel febbraio del 1996. Inoltre, per tutti gli anni in cui aveva lavorato al Veteran's Affairs Medical Center, il turno che mostrava un drastico aumento nel numero di decessi era proprio il suo. Per un profano, ciò potrebbe suggerire che Kristen Gilbert era chiaramente la responsabile delle morti, ma di per sé non sarebbe sufficiente ad assicurare la sua colpevolezza; a dire il vero, non sarebbe nemmeno sufficiente a giustificare un'accusa. Il problema è che potrebbe trattarsi di una mera coincidenza. Il compito dello statistico in questa situazione è proprio quello di determinare quanto sia improbabile una simile coincidenza. Se la risposta è che la probabilità di tale coincidenza è, poniamo, uno su cento, allora Kristen Gilbert potrebbe benissimo essere innocente. Persino una probabilità di uno su mille lascerebbe qualche dubbio sulla sua colpevolezza; ma con una probabilità di, poniamo, uno su centomila, la maggior parte della gente troverebbe le prove contro di lei piuttosto convincenti.

Per capire come funziona la tecnica del test d'ipotesi, iniziamo con il semplice esempio del lancio di una moneta. Se la moneta è perfettamente equilibrata (cioè, se non è stata truccata in modo da mostrare più frequentemente una delle due facce), la probabilità di ottenere testa è 0,5.³ Supponiamo di lanciare la moneta dieci volte per vedere se è truccata in modo da favorire il risultato «testa». A questo punto possiamo ottenere una gamma di risultati differenti, e possiamo calcolare la loro probabilità. Ad esempio, la probabilità che esca testa almeno sei volte è circa 0,38. (Il calcolo è chiaro ma un po' intricato, in quanto ci sono molti modi possibili di ottenere sei o più teste in dieci lanci e occorre tener conto di tutti.) La cifra 0,38 assegna un preciso valore numerico al fatto che, a livello intuitivo, non saremmo sorpresi se lanciando una moneta dieci volte ottenessimo sei o più teste. La probabilità di ottenere almeno sette teste è pari a 0,17, una cifra che riflette la nostra intuizione del fatto che, seppure sette o più teste sia un risultato un po' insolito, certamente non lo è abbastanza da fondare il sospetto che la moneta sia truccata. Ciò che ci sorprenderebbe è un risultato di nove teste, per il quale la probabilità si riduce a 0,01, cioè a un caso su cento. La probabilità che esca testa dieci volte in dieci lanci è circa 0,001, o uno su mille, e se ciò accadesse sospetteremmo sicuramente che la moneta sia truccata. Così, lanciando la moneta dieci volte, possiamo formulare un giudizio preciso e attendibile, basato sulla matematica, in merito all'ipotesi che la moneta non sia truccata.

Nel caso delle morti sospette al Veteran's Affairs Medical Center, gli investigatori volevano sapere se il numero di decessi verificatisi quando Kristen Gilbert era in servizio fosse così improbabile da non poter rappresentare una semplice coincidenza. La matematica coinvolta è un po' più complessa che nel caso del lancio della moneta, ma l'idea è la stessa. La tabella 1 presenta i dati che gli investigatori avevano a disposizione. Essa mostra i numeri di turni, classificati in diversi modi, e copre il periodo di diciotto mesi terminato nel febbraio del 1996, il *mese* in cui i tre infermieri palesarono le loro preoccupazioni al caporeparto e in cui Kristen Gilbert, poco dopo,

³ In realtà, questo non è del tutto corretto. A causa delle proprietà inerziali di una moneta fisica, essa tende a opporre una lieve resistenza alla rotazione, con il risultato che se si lancia una moneta perfettamente bilanciata imprimendo una forza iniziale casuale, la probabilità che essa ricada nella stessa posizione di partenza è 0,51. Ma ignoreremo questa precisazione nell'analisi che segue.

prese un permesso per malattia.

Gilbert presente	Morti durante il turno		
	Sì	No	Totale
Sì	40	217	257
No	34	1350	1384
Totale	74	1567	1641

Tabella 1. I dati per l'analisi statistica nel caso Gilbert.

Complessivamente, si erano verificati 74 decessi, distribuiti in un totale di 1641 turni. Se si assume che le morti fossero avvenute casualmente, queste cifre suggeriscono che la probabilità di un decesso in ogni turno era circa 74 su 1641, ovvero 0,045. Concentrandoci ora sui turni in cui aveva lavorato Kristen Gilbert, questi erano stati in totale 257. Se Gilbert non avesse ucciso nessun paziente, ci aspetteremmo un numero di morti durante i suoi turni pari a $0,045 \times 257 = 11,6$, cioè circa 11 o 12. In realtà i pazienti deceduti durante i suoi turni erano molti di più: per la precisione 40. Quanto è probabile questo fatto? Impiegando metodi matematici simili a quelli che abbiamo visto per i lanci della moneta, Gehlbach calcolò la probabilità che, sul totale dei 74 decessi, 40 o più fossero concentrati nei turni di Kristen Gilbert, e scoprì che essa era inferiore a uno su cento milioni. In altre parole, era estremamente improbabile che i suoi turni fossero stati semplicemente «sfortunati» per i pazienti.

Il gran giurì decise che c'erano prove sufficienti per incriminare Kristen Gilbert; presumibilmente l'analisi statistica costituì la prova più convincente, ma non lo sappiamo con sicurezza, giacché le deliberazioni delle giurie non sono di pubblico dominio. La donna fu accusata di quattro omicidi e di tre tentati omicidi. Siccome il Veteran's Affairs Medical Center è un servizio federale, il processo si tenne in un tribunale federale, anziché in uno statale, e sotto le leggi federali. Una significativa conseguenza di questo fatto fu che, sebbene il Massachusetts non abbia la pena di morte, la legge federale la prevede, e fu proprio questa la condanna che l'accusa chiese per Kristen Gilbert.

Statistica in tribunale?

Un aspetto interessante di questo caso è che il giudice federale stabilì in deliberazioni preprocessuali che le prove statistiche non dovevano essere presentate in tribunale. Nell'emettere questa ordinanza, il giudice prese nota di una teoria elaborata da un secondo statistico coinvolto nel caso, George Cobb del Mount Holyoke College.

Cobb e Gehlbach non erano in disaccordo su nessuna delle analisi statistiche (di fatto finirono per scrivere un articolo congiunto su questo caso.) A differire erano piuttosto i loro ruoli e le questioni che affrontavano. Il compito di Gehlbach era di

usare la statistica per stabilire se c'erano basi ragionevoli per sospettare che Kristen Gilbert fosse colpevole di pluriomicidio. Più specificamente, egli compì un'analisi che mostrava che l'aumento nel numero di decessi all'ospedale durante i turni in cui Kristen Gilbert era in servizio non poteva essere dovuto a una variazione casuale. Ciò bastava a fondare i sospetti che la donna fosse la causa di quell'incremento, ma non era certamente abbastanza *per provare* che le cose stavano davvero in questo modo. Quello che sosteneva Cobb era che la determinazione di una relazione statistica non spiega la causa di quella relazione. Il giudice accolse questa argomentazione, in quanto lo scopo del processo non era quello di decidere se esistevano basi per sospettare della colpevolezza di Kristen Gilbert, cosa che era già stata stabilita dal gran giuri e dall'US Attorney's Office. Piuttosto, il compito del tribunale era di stabilire se Kristen Gilbert aveva causato o meno le morti in questione. La motivazione del giudice per escludere le prove statistiche era che, come avevano dimostrato le sue esperienze in casi precedenti, i giurati che hanno scarsa dimestichezza con il ragionamento statistico - vale a dire, quasi tutti - hanno di solito molte difficoltà a capire perché una probabilità di uno su cento milioni che le morti sospette siano avvenute per caso *non* implica che anche la probabilità che Kristen Gilbert sia innocente equivalga a uno su cento milioni. La probabilità originaria potrebbe essere *causata* da qualcos'altro.

Cobb illustrò la differenza per mezzo di un famoso esempio tratto dalla lunga lotta che medici e scienziati hanno dovuto combattere per vincere sulla potente lobby del tabacco e convincere i governi e la gente che fumare sigarette causa il cancro ai polmoni. La tabella 2 mostra i tassi di mortalità per tre categorie di persone: non fumatori, fumatori di sigarette e fumatori di sigari e pipa.

Non fumatori	20,2
Fumatori di sigarette	20,5
Fumatori di sigari e pipa	35,3

Tabella 2. Tassi di mortalità per 1000 persone per anno.

A prima vista, le cifre nella tabella 2 sembrano indicare che fumare sigarette non è pericoloso mentre fumare sigari e pipa lo è. Ma le cose non stanno così. C'è una variabile cruciale che si cela dietro ai dati e che i numeri di per sé non rivelano: l'età. L'età media dei non fumatori in quell'indagine era 54,9 anni, l'età media dei fumatori di sigarette era 50,5 anni e l'età media dei fumatori di sigari e pipa era 65,9 anni. Utilizzando tecniche statistiche per tenere conto delle differenze di età, le cifre furono corrette nel modo illustrato dalla tabella 3.

Non fumatori	20,3
Fumatori di sigarette	28,3
Fumatori di sigari e pipa	21,2

Tabella 3. Tassi di mortalità per 1000 persone per anno, corretti per età.

Ora emerge un risultato molto differente, che indica che fumare sigarette è molto pericoloso.

Ogni volta che viene effettuato un calcolo delle probabilità sulla base dei dati osservativi, il massimo che in genere si può concludere è che esiste una correlazione tra due o più fattori. Ciò può essere sufficiente per stimolare ulteriori indagini, ma di per sé questo risultato non stabilisce un rapporto di causalità. C'è sempre la possibilità di una variabile nascosta che giace dietro la correlazione.

Quando viene compiuto uno studio, poniamo, sull'efficacia o la sicurezza di un nuovo farmaco o di una nuova procedura medica, gli statistici, anziché affidarsi ai dati osservativi, affrontano il problema dei parametri nascosti conducendo test randomizzati in doppio cieco. In uno studio di questo tipo, la popolazione esaminata viene suddivisa in due gruppi mediante una procedura totalmente casuale, tale per cui la ripartizione dei gruppi non è nota né ai soggetti sperimentali né a coloro che somministrano il farmaco o il trattamento (di qui l'espressione «doppio cieco»). A uno dei due gruppi viene somministrato il farmaco o il trattamento, mentre l'altro viene trattato con un placebo o con una cura fasulla. In un simile esperimento, la distribuzione casuale in gruppi annulla il possibile effetto di parametri nascosti, cosicché in questo caso una bassa probabilità che un risultato positivo sia semplicemente dovuto a variazione casuale può davvero essere presa come una prova conclusiva del fatto che il farmaco o il trattamento costituiscono la causa di quel risultato.

Nel cercare di risolvere un caso di crimine, ovviamente, non c'è altra possibilità se non quella di lavorare sui dati disponibili. Di conseguenza, usare la procedura del test d'ipotesi, come nel caso Gilbert, può essere molto utile per identificare un sospetto, ma per provarne la colpevolezza generalmente sono necessari altri mezzi.

Nel caso *Stati Uniti contro Kristen Gilbert*, l'analisi statistica di Gehlbach non fu sottoposta alla giuria, ma i giurati trovarono comunque prove sufficienti per dichiarare l'imputata colpevole di tre omicidi di primo grado, di un omicidio di secondo grado e di due tentati omicidi. Benché l'accusa avesse chiesto la condanna a morte, su questo punto la giuria si divise in quattro membri favorevoli e otto contrari, e di conseguenza Kristen Gilbert fu condannata all'ergastolo senza possibilità di rilascio sulla parola.

Sorvegliare la polizia

Un altro impiego delle tecniche statistiche di base nell'ambito dei servizi di polizia riguarda l'importante questione di assicurare che i poliziotti stessi rispettino la legge.

Agli agenti di polizia viene conferito un grande potere su tutti gli altri cittadini, e uno dei compiti della società è assicurarsi che non abusino di questo potere. In particolare, si presume che gli agenti di polizia trattino tutti in modo equo e giusto, senza pregiudizi basati su genere, etnia, condizione economica, età, modo di vestire o religione.

Ma accertare un pregiudizio è una faccenda insidiosa e, come abbiamo visto nella nostra precedente discussione sul fumo, uno sguardo superficiale ai dati statistici può

talvolta portare a conclusioni completamente errate. Ciò è illustrato in modo assai eloquente dal seguente esempio, il quale, sebbene non correlato all'attività di polizia, indica chiaramente il bisogno di accostarsi alla statistica con qualche sofisticato accorgimento matematico.

Negli anni '70 qualcuno notò che nelle selezioni per l'ammissione ai corsi di specializzazione dell'Università di California a Berkeley fu accettato il 44 per cento delle domande presentate da maschi, ma solo il 35 per cento di quelle inoltrate da candidati di sesso femminile. Sembrava un chiaro caso di discriminazione di genere e, non sorprendentemente (soprattutto a Berkeley, da tempo nota per essere sede di molti eminenti sostenitori della parità dei sessi), fu intentata una causa legale per pregiudizio di genere nelle politiche di ammissione.

Le domande di iscrizione a Berkeley non sono generiche ma vengono presentate per singoli programmi di studio - come ingegneria, fisica o inglese - e di conseguenza un eventuale favoritismo nelle ammissioni si presenterà nell'ambito di uno o più programmi particolari. La tabella 4 presenta i dati sulle ammissioni programma per programma:

Materia di specializzazione	Candidati maschi	Percentuali di ammessi	Candidati femmine	Percentuale di ammessi
A	825	62	108	82
B	560	63	25	68
C	325	37	593	34
D	417	33	375	35
E	191	28	393	24
F	373	6	341	7

Tabella 4. Cifre relative all'ammissione ai corsi dell'Università di California a Berkeley, suddivise per programma.

Se si considera ciascun programma individualmente, i candidati maschi ammessi non sembrano essere molti di più delle femmine. In realtà la percentuale di femmine ammesse al programma A, con un numero molto alto di iscrizioni, era considerevolmente superiore a quella dei maschi, e in tutti gli altri programmi le percentuali erano piuttosto vicine. Come è possibile allora che nel complesso apparisse un vantaggio per i candidati maschi?

Per rispondere a questa domanda, occorre vedere per quali programmi maschi e femmine avevano fatto domanda. I maschi avevano presentato le loro domande soprattutto per i programmi A e B, mentre le femmine si erano candidate principalmente per i programmi C, D, E e F. I programmi per cui le femmine avevano fatto domanda erano di più difficile accesso di quelli per cui si erano candidati i maschi (le percentuali di ammessi erano basse per entrambi i generi), ed è questa la ragione per cui, osservando i dati complessivi, sembrava che i maschi fossero stati avvantaggiati nelle selezioni.

C'era effettivamente in gioco un fattore di genere, ma questo non aveva nulla a che vedere con le procedure di ammissione dell'università. Piuttosto, si trattava di un fattore di autoselezione da parte degli studenti che avevano presentato domanda, per

cui le femmine avevano evitato i programmi A e B.

Il caso di Berkeley fu un esempio di un curioso fenomeno noto come paradosso di Simpson, dal nome dello studioso E.H. Simpson che lo aveva esaminato in un famoso articolo del 1951.⁴

Come si accerta l'esistenza di un pregiudizio?

Tenendo a mente l'esempio ammonitore citato sopra, come dovremmo valutare lo studio condotto a Oakland, in California, nel 2003 (dalla RAND Corporation, su richiesta della Racial Profiling Task Force del dipartimento di polizia di Oakland), per stabilire se c'era un sistematico pregiudizio razziale nel modo in cui la polizia fermava gli automobilisti?

I ricercatori della RAND esaminarono 7607 blocchi di veicoli verbalizzati dagli agenti di polizia di Oakland tra giugno e dicembre del 2003, utilizzando vari strumenti matematici per analizzare diverse variabili, in modo da portare alla luce qualunque prova potesse suggerire una discriminazione razziale. Uno dei risultati dell'indagine fu che i neri erano coinvolti nel 56 per cento di tutti i casi studiati di blocco del traffico, sebbene costituissero solo il 35 per cento della popolazione residente a Oakland.

Questo risultato indica discriminazione razziale? Be', potrebbe; ma non appena guardiamo più attentamente quali altri fattori potrebbero essere riflessi in questi numeri, la questione non è per niente chiara.

Ad esempio, come accade in molti centri urbani, alcune zone di Oakland hanno tassi di criminalità molto più elevati di altre, e la polizia pattuglia queste aree molto più frequentemente di quelle con un tasso di criminalità inferiore.

Di conseguenza, in queste zone i posti di blocco saranno più frequenti che in altre. Dal momento che solitamente le aree con più alti tassi di criminalità corrispondono alle zone in cui le minoranze etniche sono più concentrate, la più alta frequenza di arresti del traffico in queste aree si traduce necessariamente in una più alta frequenza di blocchi di veicoli guidati da automobilisti appartenenti a minoranze etniche.

Al fine di superare queste incertezze, i ricercatori della RAND escogitarono un modo particolarmente ingegnoso per individuare possibili pregiudizi razziali. Se fosse stata in atto una discriminazione razziale, ragionarono, il fermo di autisti appartenenti a minoranze etniche sarebbe stato più frequente quando fosse possibile identificarli in anticipo come tali.

Pertanto, essi confrontarono i blocchi effettuati in un arco di tempo appena prima del calar della notte con quelli compiuti al buio, quando gli agenti avevano meno probabilità di poter riconoscere l'etnia del guidatore.

Le cifre mostrarono che il 50 per cento degli automobilisti fermati durante il giorno era di pelle nera, mentre di notte i guidatori neri fermati erano il 54 per cento. Sulla base di questo risultato, non sembrava esserci un sistematico pregiudizio razziale nei

⁴ E.H. Simpson, *The Interpretation of Interaction in Contingency Tables*, in *Journal of the Royal Statistical Society*, 1951, Ser. B, n. 13, pp. 238-241.

blocchi del traffico.

Ma i ricercatori andarono un po' più a fondo ed esaminarono i rapporti degli stessi poliziotti in merito alla loro capacità di determinare l'etnia del guidatore prima di fermarlo. Nei casi in cui gli agenti dichiaravano di conoscere l'etnia del guidatore prima di fermare il veicolo, il 66 per cento degli automobilisti fermati era di pelle nera, mentre in tutti gli altri casi solo il 44 per cento. Questo è un indice piuttosto forte di pregiudizio razziale.⁵

⁵ Purtroppo, nonostante i molti sforzi fatti per eliminare il problema, quella del pregiudizio razziale da parte della polizia sembra essere una questione persistente in tutti gli Stati Uniti. Per citare solo un rapporto recente, *An Analysis of Traffic Stop Data in Riverside, California*, di Larry K. Gaines della California State University a San Bernardino, pubblicato in *Police Quarterly*, giugno 2006, n. 9, 2, pp. 210-233: «I risultati del *profiling* razziale e degli studi sui blocchi del traffico sono abbastanza coerenti: gli appartenenti a minoranze etniche, soprattutto gli afroamericani, vengono fermati, multati e perquisiti più frequentemente dei bianchi. Ad esempio, Lamberth (citato in *State v. Fedro Soto*, 1996) ha scoperto che la polizia dello Stato del Maryland fermava e perquisiva gli afroamericani con una frequenza maggiore rispetto a quella delle loro infrazioni dei limiti di velocità. Harris (1999) ha esaminato i verbali di Akron, Dayton, Toledo e Columbus, in Ohio, e ha scoperto che gli afroamericani erano citati con una frequenza che superava la loro rappresentanza nella popolazione dei guidatori. Cordner, Williams e Zuniga (2000) e Cordner, Williams e Velasco (2002) hanno rilevato tendenze simili a San Diego, in California. Zingraff e i suoi colleghi (2000) hanno analizzato i blocchi effettuati dalla polizia stradale del North Carolina e hanno scoperto che gli afroamericani erano sovrarappresentati negli episodi di fermo e di perquisizione».

DATA MINING

Trovare schemi significativi in masse di informazioni

Brutus

Charlie Eppes è seduto di fronte a una fila di computer e di monitor televisivi. Sta testando un programma informatico che ha creato per aiutare la polizia a sorvegliare le grandi folle, cercando comportamenti insoliti che potrebbero indicare un imminente atto criminale o terroristico. La sua idea è di usare le ordinarie equazioni matematiche che descrivono il comportamento dei fluidi in fiumi, laghi, oceani, cisterne, tubature e persino nei vasi sanguigni.⁶ Sta sperimentando il nuovo sistema a un ricevimento per la raccolta di fondi per un senatore californiano. Telecamere monitorano gli invitati dall'alto mentre si muovono per la stanza, e il programma informatico di Charlie analizza il «flusso» delle persone. Improvvisamente l'esperimento prende una piega inattesa. L'FBI riceve una telefonata che avverte che un uomo armato si trova nella stanza, con l'intenzione di uccidere il senatore.

Il software funziona e Charlie riesce a identificare il sicario, ma Don e la sua squadra non riescono a impedirgli di sparare al senatore e poi rivolgere la pistola contro se stesso.

Si scopre che l'assassino era un immigrato vietnamita, ex guerrigliero vietcong, che, sebbene fosse stato in prigione in California, in qualche modo era riuscito a ottenere la cittadinanza americana e a ricevere una regolare pensione dall'esercito statunitense. La sera dell'omicidio aveva anche preso dello *speed*, una droga illegale. Mentre Don sta facendo qualche indagine per capire cosa stia succedendo, riceve la visita di un agente della CIA che gli chiede aiuto per evitare un'eccessiva fuga di informazioni riguardo al caso. A quanto sembra l'assassino morto era stato parte di un progetto segreto di modificazione del comportamento condotto dalla CIA nelle prigioni della California nel corso degli anni '60, che mirava a trasformare i detenuti in sicari addestrati a svolgere un compito assegnato, una volta resi operativi, e poi a uccidersi. (Purtroppo, questa idea non è meno bizzarra di quella di Charlie di usare le equazioni che descrivono il flusso dei fluidi per studiare il comportamento delle folle.)

Ma perché questo particolare individuo è improvvisamente entrato in azione uccidendo il senatore?

Il quadro si fa molto più chiaro quando avviene un secondo omicidio. La vittima questa volta è un celebre psichiatra e l'assassino un immigrato cubano. Anche lui aveva trascorso del tempo in una prigione della California e riceveva regolari assegni pensionistici dall'esercito. Ma in questo caso, quando l'assassino cerca di togliersi la

⁶ L'idea si basa su diversi progetti reali che cercano di usare le equazioni che descrivono il comportamento dei fluidi per analizzare vari tipi di attività di massa, come il flusso del traffico sulle autostrade, le folle di spettatori che entrano ed escono da un grande stadio, e le uscite di emergenza da un edificio in caso di incendio.

vita dopo aver ucciso la vittima, la pistola si inceppa ed egli è costretto a fuggire dalla scena del delitto. L'identificazione delle impronte digitali lasciate sulla pistola porta in breve tempo al suo arresto.

Quando Don scopre che il senatore morto aveva sollecitato l'abrogazione del divieto statale di usare tecniche di modificazione del comportamento sui carcerati, e che lo psichiatra assassinato aveva raccomandato di riadottare tali tecniche per sopprimere le tendenze criminali, conclude rapidamente che qualcuno ha iniziato ad aizzare gli assassini condizionati contro le stesse persone che stavano facendo pressione per il riutilizzo delle tecniche che li avevano prodotti. Ma chi?

Don pensa che la migliore linea di indagine sia di scoprire chi ha fornito le pistole usate dai due assassini. Si sa che le armi arrivano da un fornitore nel Nevada. Charlie riesce a compiere il passo successivo, che conduce all'identificazione dell'individuo che si cela dietro i due omicidi. Egli ricava i dati su tutte le vendite di pistole in cui era coinvolto quel particolare fornitore e analizza le relazioni tra tutte le vendite che hanno avuto origine lì. Spiega che sta impiegando tecniche matematiche simili a quelle usate per analizzare gli schemi di chiamate sulla rete telefonica: un approccio adottato frequentemente nelle vere indagini poliziesche.

Questo è ciò che gli spettatori hanno visto nell'episodio della terza serie di *NUMB3RS* intitolato *Brutus* (il nome in codice per il fittizio progetto di condizionamento degli assassini messo in atto dalla CIA), mandato in onda per la prima volta negli Stati Uniti il 24 novembre 2006. Come sempre, la matematica che Charlie utilizza nella rappresentazione televisiva è basata sulla vita reale.

Il metodo impiegato da Charlie per rintracciare la distribuzione delle armi da fuoco è generalmente chiamato *link analysis* (analisi di legame), ed è una delle tante tecniche che vanno sotto il nome collettivo di *data mining* (estrazione dai dati). Il *data mining* è utilizzato per ottenere informazioni utili dalla massa di dati a disposizione - spesso pubblicamente - nella società moderna.

Trovare significato nelle informazioni

Le tecniche di *data mining* furono originariamente messe a punto dall'industria della vendita al dettaglio per individuare i comportamenti di acquisto dei clienti. (Vi siete mai chiesti perché i supermercati offrano ai clienti tutte queste carte fedeltà - a volte chiamate carte «club» - in cambio di sconti? In parte è per incoraggiare i clienti a continuare a comprare nello stesso negozio, ma per questo basterebbero prezzi bassi. Il fattore importante per la compagnia è che esse consentono di individuare comportamenti di acquisto dettagliati collegabili ai codici di avviamento postale dei clienti, informazioni che possono poi essere analizzate con le tecniche di *data mining*.)

Sebbene una gran parte del lavoro nel *data mining* sia svolto dai computer, perlopiù questi computer non operano in maniera autonoma. Anche l'esperienza umana ricopre un ruolo significativo, e una tipica indagine di *data mining* implica una costante interazione tra uomo e macchina.

Molte delle applicazioni informatiche impiegate nel *data mining* cadono nell'area

generale nota come intelligenza artificiale, un'espressione che però può essere fuorviante, in quanto suggerisce l'idea di computer che pensano e agiscono come le persone. Anche se negli anni '50, quando furono condotti i primi esperimenti di intelligenza artificiale, molti pensavano che quella fosse una possibilità concreta, alla fine divenne chiaro che una cosa simile non si sarebbe realizzata nell'immediato futuro, e forse mai. Ma tale consapevolezza non impedì la creazione di molti programmi di «ragionamento automatizzato», alcuni dei quali alla fine trovarono un uso efficace e importante nel *data mining*, dove l'esperto umano spesso fornisce l'«intelligenza di alto livello» necessaria a guidare il programma informatico che svolge il grosso del lavoro. In questo modo, il *data mining* offre un esempio eccellente delle potenzialità che emergono quando cervello umano e computer cooperano tra loro.

Tra i principali metodi e strumenti usati nel *data mining* vi sono:

- analisi di legame (link analysis): ricerca di associazioni e di altre forme di connessione tra, poniamo, criminali o terroristi;
- raggruppamento geometrico (geometrie clustering): una forma specifica di analisi di legame;
- agenti software (software agents): piccoli pezzi autonomi di codice informatico che possono monitorare, recuperare, analizzare e agire sulle informazioni;
- apprendimento automatico (machine learning): algoritmi che sono in grado di estrarre profili di criminali e mappe grafiche di crimini;
- reti neurali (neural networks): speciali tipi di programmi informatici capaci di prevedere la probabilità di crimini e di attacchi terroristici.

Vediamo brevemente in che cosa consiste ognuno di questi metodi.

Analisi di legame

I giornali spesso si riferiscono all'analisi di legame con l'espressione «connettere i punti». Si tratta del processo con cui vengono ricostruite le connessioni tra persone, eventi, luoghi e organizzazioni. Tali connessioni potrebbero essere legami di famiglia, rapporti di affari, associazioni criminali, transazioni finanziarie, incontri tra persone, scambi di e-mail e molte altre cose. L'analisi di legame può essere particolarmente utile nella lotta contro il terrorismo, il crimine organizzato, il riciclaggio di denaro (*follow the money*) e le frodi telefoniche.

L'analisi di legame è principalmente un processo guidato da un esperto umano. La matematica e la tecnologia vengono utilizzate per munire un esperto di strumenti informatici potenti e flessibili che lo aiutino a scoprire, esaminare e ricostruire possibili connessioni. Tali strumenti generalmente consentono all'analista di rappresentare i dati collegati come una rete, mostrata ed esaminata (del tutto o in parte) sullo schermo del computer, nella quale i nodi rappresentano gli individui, le organizzazioni o i luoghi di interesse e i collegamenti tra i nodi indicano le relazioni o le transazioni. Gli strumenti possono anche permettere all'analista di indagare e registrare dettagli relativi a ciascun collegamento, e di scoprire nuovi nodi che si

connettono a quelli già visti o nuovi legami tra i nodi preesistenti.

Ad esempio, in un'indagine condotta su una sospetta cerchia di criminali, un investigatore potrebbe compiere un'analisi di legame delle telefonate che un sospetto ha effettuato o ricevuto, ricavabili dal registro delle chiamate della compagnia telefonica, facendo attenzione a fattori come il numero chiamato, l'orario e la durata di ciascuna telefonata o il numero chiamato nella telefonata successiva. L'investigatore potrebbe quindi decidere di ampliare l'analisi della rete delle chiamate esaminando le telefonate effettuate e ricevute da uno o più individui con i quali il sospetto iniziale aveva avuto conversazioni telefoniche. Questo processo può portare all'attenzione dell'investigatore individui in precedenza sconosciuti. Alcuni potrebbero dimostrarsi del tutto innocenti, ma altri potrebbero risultare membri di un'organizzazione criminale.

Un'altra linea di indagine può essere quella di seguire le transazioni di denaro verso e da conti bancari nazionali e internazionali.

Un'altra linea ancora può essere di esaminare la rete di luoghi e individui visitati dal sospetto, servendosi di dati come acquisti di biglietti ferroviari e aerei, punti di arrivo e di partenza da un dato Paese, noleggi di automobili, operazioni di acquisto con carte di credito, siti Internet visitati e cose simili.

Dato che oggi è pressoché impossibile fare qualcosa senza lasciare una traccia elettronica, la sfida che l'analisi di legame deve affrontare solitamente non è quella di avere dati insufficienti, bensì di decidere quali dati, tra tutti i megabyte disponibili, debbano essere selezionati per le analisi successive. L'analisi di legame funziona meglio quando è sostenuta da altri tipi di informazioni, come le soffiare provenienti dagli informatori della polizia o dai vicini di casa di un possibile sospetto.

Una volta che un'analisi di legame iniziale ha identificato una possibile rete di criminali o di terroristi, è possibile determinare l'identità dei membri principali esaminando quali individui abbiano più collegamenti con gli altri componenti della rete.

Raggruppamento genetico

A causa delle risorse limitate di cui dispongono, le forze di polizia di solito si concentrano principalmente sui crimini più grossi, con il risultato che le trasgressioni minori, come i taccheggi o i furti nelle case, ricevono scarsa considerazione. Ma se un singolo o una banda organizzata commette regolarmente molti crimini del genere, il loro insieme complessivo può costituire un'attività criminale significativa che merita maggiore attenzione da parte della polizia. Il problema che si pone alle autorità, allora, è di identificare, nel gran numero di crimini minori che avvengono ogni giorno, gli insiemi che sono opera di un singolo individuo o di una banda.

Un esempio di crimine «minore» spesso perpetrato in modo regolare da due (talvolta tre) complici è il furto in una casa realizzato con il pretesto di una finta visita ufficiale (*bogus official burglary* o *distraction burglary*). Si ha quando due persone si presentano al portone di una casa (i bersagli preferiti sono spesso gli anziani) fingendosi funzionari di qualche tipo - tecnici telefonici, rappresentanti di un'impresa

di pubblici servizi o agenti governativi locali - e, mentre uno dei due distrae il padrone di casa, l'altro si muove rapidamente per l'abitazione prendendo tutti i soldi e gli oggetti di valore facilmente accessibili.

Le vittime di questi furti spesso denunciano il crimine alla polizia, la quale poi manda un suo agente nella casa interessata per stendere un rapporto. Dato che la vittima ha passato molto tempo con uno dei ladri (quello che lo ha distratto), il rapporto includerà spesso una descrizione piuttosto dettagliata di questo individuo - genere, etnia, altezza, costituzione, età approssimativa, aspetto generale del volto, occhi, colore, lunghezza e taglio di capelli, accento, segni fisici particolari, maniere, scarpe, abbigliamento, gioielli insoliti ecc. - unitamente al numero di complici e al loro genere. In linea di principio, tale ricchezza di informazioni rende i crimini di questo tipo ideali per l'utilizzo del *data mining*, e in particolare della tecnica nota come *raggruppamento geometrico*, al fine di identificare i gruppi di crimini perpetrati da una singola banda. L'applicazione di tale metodo è, tuttavia, irta di difficoltà e finora esso sembra aver funzionato solo in uno o due studi sperimentali. Prenderemo in esame uno di questi studi, sia per mostrare come funziona il metodo sia per illustrare alcuni dei problemi spesso incontrati dai professionisti del *data mining*.

Il seguente studio fu compiuto in Inghilterra nel 2000 e nel 2001 da alcuni ricercatori dell'Università di Wolverhampton in collaborazione con la West Midlands Police.⁷ Furono esaminati i rapporti delle vittime di furti in casa con aggiro effettuati in quel distretto di polizia in un periodo di tre anni. Nel corso di quel periodo, erano stati registrati 800 casi che coinvolgevano 1292 trasgressori. Questo numero risultò troppo grande per le risorse disponibili e l'analisi fu quindi limitata ai casi in cui a distrarre la vittima era stato un individuo di sesso femminile, un gruppo comprendente 89 crimini e 105 descrizioni di perpetratori.

Il primo problema fu che le descrizioni dei colpevoli si presentavano per la maggior parte nella forma narrativa in cui erano state scritte dall'agente investigativo che aveva raccolto le dichiarazioni della vittima. Per mettere le descrizioni in una forma strutturata, si dovette ricorrere a una tecnica di *data mining* nota come *text mining* (estrazione dal testo). A causa dei limiti del software disponibile per il *text mining*, fu necessario affidarsi all'intervento umano per gestire molti dei dati in ingresso come, ad esempio, errori di ortografia, abbreviazioni più o meno intuitive («Bham» o «B'ham» per «Birmingham») e modi differenti per esprimere la stessa cosa («accento di Birmingham», «accento di Bham», «accento locale», «accento: locale» ecc.).

Dopo qualche analisi iniziale, i ricercatori decisero di concentrarsi su otto variabili: età, altezza, colore e lunghezza dei capelli, corporatura, accento, etnia e numero di complici.

Una volta processati i dati in un formato adeguatamente strutturato, il passo successivo fu di usare la tecnica di *raggruppamento geometrico* per riunire le 105 descrizioni di trasgressori in insiemi che si riferivano probabilmente al medesimo individuo. Per capire come fu effettuato questo raggruppamento, iniziamo considerando un metodo che a prima vista potrebbe apparire valido, ma che presto

⁷ Si veda R. Adderley e P.B. Musgrove, *General Review of Police Crime Recording and Investigation Systems*, in *Policing: An International Journal of Police Strategies and Management*, 2001, n.24(1), pp. 110-114.

dimostra di avere notevoli difetti. Poi, vedendo come si possono correggere questi difetti, arriveremo al metodo impiegato nello studio inglese.

Per prima cosa, traduciamo ciascuna delle otto variabili in numeri. L'età - spesso un'ipotesi - è probabilmente indicata con un numero o come un intervallo; se è espressa da un intervallo, prendiamo il valore medio. Il genere (non considerato nello studio del British Midlands perché in tutti i casi esaminati l'individuo che aveva distratto la vittima era di sesso femminile) può essere indicato con il numero 1 per i maschi e con 0 per le femmine. L'altezza può essere espressa da un numero (centimetri), da un intervallo o da un termine come «alto», «medio» o «basso»; di nuovo deve essere scelto qualche metodo per convertire ognuno di questi dati in un unico numero. Allo stesso modo, occorre ideare degli schemi che rappresentino ognuna delle altre variabili come un numero.

Una volta ultimata la traduzione numerica, ciascuna descrizione dei colpevoli viene rappresentata da un vettore a otto componenti, le coordinate di un punto in uno spazio geometrico (euclideo) a otto dimensioni. La comune misura della distanza nella geometria euclidea (metrica pitagorica) può quindi essere usata per misurare la distanza geometrica tra tutte le coppie di punti. In questo modo, la distanza tra due vettori $(x_1, \dots, x_8)$ e $(y_1, \dots, y_8)$ sarà:

$$\sqrt{[(x_1 - y_1)^2 + \dots + (x_8 - y_8)^2]}$$

I punti che risultano vicini in base a questa metrica corrispondono probabilmente a descrizioni di perpetratori con molte caratteristiche in comune; e più i punti sono vicini, maggiore è il numero delle caratteristiche che le descrizioni hanno probabilmente in comune. (Ricordiamo che questo approccio presenta alcuni problemi, di cui parleremo tra poco. Per il momento, supponiamo che le cose funzionino più o meno come abbiamo appena descritto.)

La sfida ora è di identificare gruppi di punti vicini tra loro. Se ci fossero solo due variabili, sarebbe facile. Tutti i punti potrebbero essere raffigurati su un unico grafico x, y e la semplice ispezione a occhio nudo indicherebbe i possibili gruppi. Ma gli esseri umani non sono assolutamente in grado di visualizzare uno spazio a otto dimensioni, per quanto grande possa essere l'aiuto fornito dai progettisti di sistemi software per mezzo degli strumenti di visualizzazione dei dati. Il modo per aggirare questa difficoltà è ridurre il vettore di punti a otto dimensioni (le descrizioni) a uno a due dimensioni (matrice o tabella). L'idea è di disporre i punti di dati (vale a dire, il vettore rappresentante le descrizioni dei trasgressori) in una griglia bidimensionale in modo che:

- le coppie di punti che sono estremamente vicine nello spazio a otto dimensioni siano inserite nella stessa entrata della griglia;
- le coppie di punti che sono attigue nella griglia siano vicine nello spazio a otto dimensioni;
- i punti più lontani nella griglia lo siano anche nello spazio a otto dimensioni.

Ciò può essere fatto utilizzando un tipo speciale di programma informatico noto

come mappa autorganizzante (*self-organizing map*, o SOM) di Kohonen, un tipo particolare di rete neurale. Le reti neurali (comprese le SOM) verranno descritte più avanti nel capitolo. Per ora, ci basti sapere che questi sistemi, operanti in maniera iterativa, sono ideali per dare origine (nel corso di numerose iterazioni) a schemi come i gruppi geometrici del tipo cui siamo interessati, e che pertanto possono effettivamente prendere un vettore a otto dimensioni come quello descritto sopra e collocare appropriatamente i punti in una griglia bidimensionale. (Parte dell'abilità necessaria per usare una SOM in maniera efficace in un caso come questo è decidere in anticipo, o attraverso qualche esperimento iniziale per prove ed errori, quali siano le dimensioni ottimali della griglia finale. Per iniziare a lavorare, la SOM necessita di questa informazione.)

Una volta che i dati sono stati immessi nella griglia, gli agenti di polizia possono esaminare le celle della griglia che contengono diverse entrate di dati, provenienti molto probabilmente da un'unica banda responsabile di una serie di crimini, e possono identificare visivamente gruppi di punti sulla griglia, anch'essi probabilmente associati all'attività di una banda. In entrambi i casi, gli agenti possono esaminare i rapporti originari corrispondenti, alla ricerca di qualcosa che indichi che quei crimini sono in effetti opera di un'unica banda.

Vediamo ora che errori ci sono nel metodo appena descritto e come fare a correggerli.

Il primo problema è che l'iniziale traduzione dei dati in numeri non è sistematica. Ciò può portare a una situazione in cui una variabile domina su altre quando i dati sono raggruppati utilizzando la distanza geometrica (la metrica pitagorica) nello spazio a otto dimensioni. Ad esempio, una dimensione che misura l'altezza (che potrebbe essere qualcosa tra 152 e 193 centimetri) determinerebbe il dato relativo al genere (0 o 1). Pertanto il primo passo è rendere confrontabili (in termini matematici, *normalizzare*) le otto variabili numeriche, in modo che ognuna vari tra 0 e 1.

Un modo per farlo potrebbe essere di dividere semplicemente ciascuna variabile per un fattore di scala appropriato per quella particolare caratteristica (altezza, età ecc.). Ma ciò introduce ulteriori problemi nel momento in cui vengono calcolate le distanze di separazione; ad esempio, se genere e altezza sono tra le variabili, allora, supponendo che tutte le altre variabili siano grossomodo le stesse, una donna molto alta finirà vicino a un uomo molto basso (perché femmina equivale a 0 e maschio a 1, mentre alto si traduce in un valore vicino a 1 e basso in uno vicino a 0). Pertanto, è necessario impiegare una procedura di normalizzazione più sofisticata.

L'approccio che fu alla fine adottato dallo studio del British Midlands consistette nel rendere binario ogni dato numerico (0 o 1). Per fare questo si dovettero suddividere le variabili continue (età e altezza) in intervalli coincidenti agli estremi (di qualche anno e di qualche centimetro, rispettivamente), in modo che 1 denotasse un dato entro un determinato intervallo e 0 significasse esterno all'intervallo, e usare coppie di variabili binarie per codificare ogni fattore di colore e lunghezza dei capelli, costituzione, accento ed etnia. L'esatta codificazione che fu scelta era piuttosto specifica per i dati in esame, ed è pertanto di scarsa utilità fornire qui tutti i dettagli. (Gli intervalli di età e di altezza furono scelti in modo che combaciassero agli estremi al fine di render conto dei dati prossimi ai limiti degli intervalli scelti.) Il processo di

normalizzazione diede come risultato un insieme di 46 variabili binarie. Pertanto, il raggruppamento geometrico fu effettuato su uno spazio a 46 dimensioni.

Un altro problema era quello di gestire i dati mancanti. Ad esempio, come fare se la dichiarazione di una vittima non dice nulla in merito all'accento del perpetratore? Immettere uno 0 significherebbe assegnare un accento. Ma che cosa succede se nel programma di raggruppamento un dato non viene introdotto? (Nello studio del British Midlands, il programma avrebbe trattato un dato mancante come uno 0.) I punti di dati mancanti sono in effetti uno dei più grossi grattacapi per gli esperti di *data mining*, e non esiste una buona soluzione universalmente accettata. Se ci sono solo pochi casi di questo tipo, li si può ignorare oppure si può vedere quali soluzioni si ottengono immettendo diversi valori.

Come accennato prima, una decisione cruciale che occorre prendere prima di mettere in funzione la SOM riguarda le dimensioni della griglia bidimensionale risultante. Essa deve essere abbastanza piccola da far sì che la SOM sia costretta a inserire alcuni punti di dati nelle stesse celle, e dia anche come risultato qualche cella non vuota con celle vicine non vuote. Gli investigatori coinvolti nello studio del British Midlands alla fine decisero di optare per una griglia con cinque righe e sette colonne. Con 105 descrizioni di criminali, la SOM fu costretta a creare diverse aggregazioni di dati.

A conclusione dello studio, agenti di polizia esperti esaminarono i risultati e li confrontarono con le dichiarazioni originarie delle vittime e con altre informazioni pertinenti (come la vicinanza geografica dei crimini in un breve lasso temporale, un altro potenziale indice di attività organizzata, non usato nell'analisi di raggruppamento) per stabilire se il processo aveva funzionato bene. Anche se tutte le parti coinvolte dichiararono che aveva avuto successo, la mole significativa di ore di lavoro per persona richiesta indica che tali metodi necessitano di uno sviluppo ulteriore, e di una maggiore automatizzazione dei vari passaggi, prima che possano essere comunemente usati per combattere un'attività criminale come quella su cui si era concentrato questo studio. Tuttavia, il metodo può essere usato per individuare raggruppamenti in altri generi di attività criminale, come il terrorismo. In questi casi, quando la posta in gioco è così alta, potrebbe valere la pena di investire una grande quantità di risorse umane ed economiche per far funzionare il metodo.

Agenti software

Gli agenti software, un prodotto della ricerca sull'intelligenza artificiale, sono sostanzialmente programmi informatici autosufficienti (e, in genere, relativamente piccoli) progettati per raggiungere specifici obiettivi, e che operano in modo autonomo, rispondendo ai cambiamenti nell'ambiente in cui lavorano. La loro autonomia è un risultato del fatto che essi incorporano una gamma di azioni differenti che possono intraprendere, a seconda dei particolari input che ricevono. In parole povere, essi includono un gran numero di istruzioni se/allora. Ad esempio, il FinCEN, un'agenzia dipendente dal dipartimento del Tesoro degli Stati Uniti che ha il compito di individuare il riciclaggio di denaro, esamina qualunque transazione di

denaro oltre i diecimila dollari. Siccome avvengono circa dieci milioni di transazioni di questo tipo ogni anno, il controllo non può essere effettuato manualmente. Pertanto, l'agenzia utilizza agenti software per realizzare il monitoraggio automaticamente, impiegando anche analisi di legame per individuare attività insolite che potrebbero indicare una frode.

Le banche utilizzano agenti software per monitorare le attività delle carte di credito, alla ricerca di un insolito andamento nelle spese che potrebbe indicare una carta rubata. (Potrebbe esservi capitata l'esperienza di vedere la vostra carta di credito rifiutata quando avete provato a usarla in nuove circostanze, come in una città o in un Paese straniero dove si erano verificate - molto probabilmente a vostra insaputa - recenti frodi con le carte di credito.)

Il dipartimento della Difesa, come altre organizzazioni governative e non governative statunitensi, ha investito grandi somme di denaro nella creazione di agenti software per la raccolta e l'analisi delle informazioni. Generalmente, la strategia consiste nel mettere a punto un sistema coordinato di agenti comunicanti tra loro, ognuno dei quali è progettato per svolgere una particolare sottofunzione. Ad esempio, un sistema coordinato di sorveglianza avente lo scopo di avvertire in anticipo di un possibile attacco biologico potrebbe includere i seguenti componenti:

- agenti che ricevono e mettono in relazione gli elementi provenienti da differenti banche dati;
- agenti che estraggono informazioni potenzialmente rilevanti da queste banche dati;
- agenti che analizzano dati selezionati e vanno alla ricerca di schemi insoliti di eventi biologici;
- agenti che classificano le anomalie e identificano patogeni specifici;
- agenti che lanciano l'allarme al personale delle unità di emergenza.

I dati esaminati inizialmente potrebbero comprendere i rapporti dei medici o i sintomi dei pazienti, le cartelle cliniche ambulatoriali, i dati dei medici scolastici o quelli relativi alle vendite di particolari farmaci. In ciascun caso, un'improvvisa deviazione da un andamento stabilito potrebbe essere dovuta a un'epidemia naturale, ma potrebbe anche rappresentare il primo segnale di un attacco biologico. Gli esseri umani non sarebbero in grado di riassumere le masse di dati e di esaminare i risultati in modo da individuare un cambiamento abbastanza rapidamente da consentire contromisure tempestive. Per fare questo è necessario ricorrere ai software.

Apprendimento automatico

Nell'arsenale delle tecniche di *data mining* a disposizione delle forze di polizia, l'apprendimento automatico, un'altra branca dell'intelligenza artificiale, costituisce forse lo strumento più importante per delineare il profilo di criminali e terroristi (e quindi, auspicabilmente, per catturarli e prevenirne le attività).

Gran parte del potere degli algoritmi di apprendimento automatico scaturisce dal fatto che essi automatizzano il processo di ricerca e identificazione di caratteristiche

chiave entro masse di dati. Si tratta di qualcosa che una persona allenata può fare - di solito meglio, a dire il vero - ma solo con piccole quantità di dati. Gli algoritmi di apprendimento automatico sono capaci di trovare il proverbiale ago nel pagliaio.

Ad esempio, se voleste scoprire un insieme di caratteristiche tipiche di un terrorista o di un narcotrafficante, potreste applicare un appropriato sistema di apprendimento automatico - uno dei tanti disponibili in commercio - a una banca dati di terroristi o narcotrafficanti noti (ovvero, già arrestati).

Seguendo qualche input iniziale fornito da voi per determinare la gamma di caratteristiche possibili, il software interrogherebbe la banca dati più o meno come avviene nel classico gioco delle venti domande. Il risultato di questo processo potrebbe essere un elenco di condizioni se/allora, ciascuna con associata una stima di probabilità, che fornisce la base per un programma - magari da usare nei posti di frontiera - che controllerà i sospetti per vedere se è probabile che stiano contrabbandando droghe. In alternativa, il processo di interrogazione della banca dati potrebbe generare un albero decisionale che può essere analogamente utilizzato come base per un programma che avvisa gli agenti di polizia di possibili terroristi o narcotrafficanti.

Il primo stadio di questo processo può essere più facilmente compreso con un esempio. Supponiamo che vogliate che il sistema di apprendimento automatico predica se un dato oggetto sia una mela, un'arancia o una banana. Potreste iniziare dicendogli di considerare peso, forma e colore. Il sistema scorre il suo elenco di oggetti appropriati - in questo caso, i frutti - e per prima cosa ne controlla il peso. Scopre quindi che questa caratteristica non permette di classificare i tre frutti. A questo punto, il sistema ricontrolla la lista esaminando la forma. Questa caratteristica consente di distinguere una banana dagli altri due frutti (cilindrica/incurvata contro sferica) ma non basta comunque per identificare il frutto. Dinanzi a un oggetto di prova, il controllo in base alla forma darebbe l'output

BANANA 100%

se l'oggetto fosse una banana, ma

MELA 50%

ARANCIA 50%

negli altri casi. Alla fine il sistema controlla il colore e questa volta scopre che la caratteristica permette di distinguere i tre frutti con un grado di accuratezza del cento per cento.

Quando un algoritmo di apprendimento automatico viene fatto lavorare su una grande banca dati di esempi passati, può spesso generare una breve lista di controllo o un albero decisionale che una guardia di frontiera o un agente di polizia può far scorrere al sistema in tempo reale per determinare la possibile o probabile colpevolezza di un sospetto criminale o terrorista. Sulla base della probabilità complessiva della colpevolezza del sospetto, il sistema può persino consigliare all'agente l'azione da intraprendere, da «lasciare andare» ad «arrestare immediatamente».

Ad esempio, benché i sistemi effettivamente impiegati non vengano resi pubblici, sembra altamente probabile che un individuo che cerca di entrare negli Stati Uniti

venga trattenuto per un ulteriore interrogatorio se presenta le seguenti caratteristiche:

ETÀ:	20-25
GENERE:	maschio
NAZIONALITÀ:	saudita
STATO DI RESIDENZA:	Germania
VISTO DI SOGGIORNO:	studente
UNIVERSITÀ:	sconosciuta
NUMERO DI INGRESSI NEL PAESE NELL'ANNO PASSATO	3
NAZIONI VISITATE NEGLI ULTIMI TRE ANNI:	Gran Bretagna, Pakistan
LEZIONI DI VOLO:	Sì

Sulla base delle prime sette caratteristiche, il sistema probabilmente suggerirebbe soltanto all'agente di compiere qualche indagine ulteriore, ma le ultime due verosimilmente provocherebbero un intervento più sostanziale. (Si può immaginare che l'ultima caratteristica venga attivata solo quando molte delle precedenti accrescono la probabilità che l'individuo sia un terrorista.)

Naturalmente, il precedente esempio non è che una grossolana semplificazione per illustrare l'idea generale. Il potere dell'apprendimento automatico è la sua capacità di costruire profili piuttosto complessi che sfuggirebbero a un agente umano. Inoltre, utilizzando metodi bayesiani (si veda il capitolo 6) per aggiornare le probabilità, il sistema può assegnare una probabilità a ciascuna conclusione. Nell'esempio precedente, il profilo potrebbe fornire queste indicazioni:

VALUTAZIONE: Possibile terrorista (probabilità 29%)

AZIONE: Trattenere e segnalare

Sebbene il nostro esempio sia fittizio, i sistemi di apprendimento automatico sono usati quotidianamente dalle guardie di frontiera e dalle forze di polizia quando passano al vaglio le persone che entrano nel Paese per scoprire eventuali attività terroristiche o traffici di droga. L'individuazione delle frodi finanziarie è un'altra delle aree in cui le forze di polizia ricorrono all'apprendimento automatico. Anche il mondo degli affari fa un ampio uso di tali sistemi, in aree come il marketing, le ricerche sui consumi e sulle esigenze dei clienti, il controllo di qualità, la gestione della catena di fornitori e così via, mentre i principali partiti politici li utilizzano per stabilire dove e come indirizzare le loro campagne.

In alcune applicazioni, i sistemi di apprendimento automatico operano come quelli descritti prima; altri fanno uso delle reti neurali, di cui parleremo ora.

Reti neurali

Il *Washington Post* del 12 giugno 2006 mostrava una pubblicità a piena pagina della Visa Corporation, in cui la compagnia annunciava che il numero di frodi con le sue carte di credito era vicino al minimo storico, e citava le reti neurali come la

principale misura di sicurezza che aveva adottato per fermare le truffe. Il successo ottenuto dalla Visa arrivò al termine di un lungo periodo di sviluppo di misure antifrode preventive basate sulle reti neurali che era iniziato nel 1993, quando la compagnia aveva sperimentato per prima l'uso di tali sistemi per ridurre l'incidenza delle truffe con le carte di credito. L'idea era che analizzando i comportamenti tipici di acquisto con le carte di credito, uno strumento di gestione del rischio basato sulle reti neurali avvertirebbe subito le banche al verificarsi di qualunque attività sospetta, in modo che esse possano informare i loro clienti se sembra che una carta sia stata usata da una persona diversa dal suo legittimo proprietario. L'individuazione delle frodi con le carte di credito è soltanto una delle molte applicazioni di *data mining* che coinvolgono l'uso di una rete neurale. Che cosa sono esattamente le reti neurali e come funzionano?

Una rete neurale è un tipo particolare di programma informatico, creato originariamente per cercare di imitare il modo in cui funziona il cervello umano. Si tratta in sostanza di una simulazione al computer di un circuito complesso attraversato da corrente elettrica (figura 2).

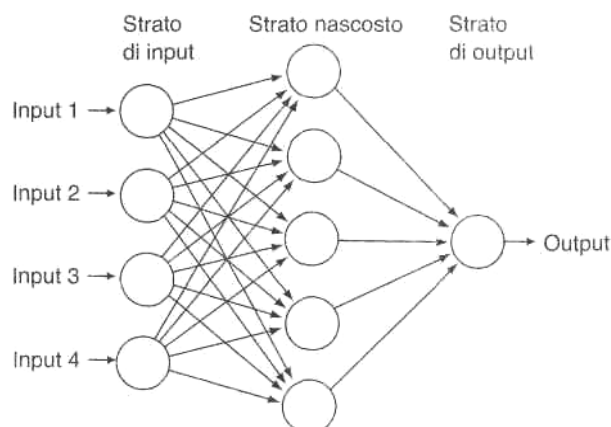


Figura 2. Una semplice rete neurale con un unico strato nascosto e un singolo nodo di output.

Le reti neurali sono particolarmente adatte a riconoscere le regolarità, e furono introdotte nel mercato negli anni '80 per compiti quali classificare le richieste di prestiti secondo il grado di rischio, distinguere le transazioni finanziarie legittime da quelle fraudolente, individuare possibili furti di carte di credito, riconoscere firme e identificare gli andamenti degli acquisti nei supermercati. Le forze di polizia iniziarono a utilizzare le reti neurali poco tempo dopo, applicandole a compiti come riconoscere un'«impronta digitale» indicante che differenti casi di incendio doloso sono probabilmente opera di un singolo individuo, o individuare attività e schemi comportamentali che indicano la possibile attività di terroristi o contrabbandieri.

Per entrare un po' più nel dettaglio della tecnologia, una rete neurale consiste di⁸ molti nodi (normalmente diverse centinaia o migliaia) sistemati in due o più «strati paralleli», in modo tale che ciascun nodo di uno strato sia connesso a uno o più nodi dello strato adiacente. Uno dei due strati terminali è lo strato di input, mentre l'altro è lo strato di output. Tutti gli altri strati sono chiamati strati intermedi o nascosti.

⁸ In realtà è più corretto dire «può essere vista come» piuttosto che «consiste di», dal momento che l'intera «rete neurale» è simulata su un normale computer digitale.

(L'idea del modello cerebrale è che i nodi simulino i neuroni e le connessioni i dendriti.) La figura 2 illustra l'idea generale, anche se una rete con così pochi nodi sarebbe di scarsa utilità pratica.

La rete comincia un ciclo operativo quando un insieme di segnali d'ingresso viene immesso nei nodi dello strato di input. Ogni volta che un nodo in qualunque punto della rete riceve un segnale d'ingresso, esso invia segnali di uscita a tutti i nodi dello strato successivo con cui è connesso. Il ciclo termina quando i segnali si sono propagati per tutta la rete e uno o più segnali di uscita emergono dal nodo di output (o dai molteplici nodi dello strato di output se la rete è strutturata in questo modo). Ciascun segnale d'ingresso e ogni segnale che emerge da un nodo possiede una certa «forza di segnale» (espressa da un numero tra 1 e 100). Ciascuna connessione internodale possiede una «forza di trasmissione» (anch'essa espressa da un numero), e la forza del segnale che passa lungo una connessione è una funzione del segnale in corrispondenza del nodo d'inizio e della forza di trasmissione della connessione. Ogni volta che un segnale è trasmesso lungo una connessione, la forza di quella connessione (spesso chiamata anche il suo «peso») aumenta o diminuisce proporzionalmente alla forza del segnale, secondo una formula prefissata. (Ciò corrisponde al modo in cui, nel cervello di un essere vivente, le esperienze della vita si traducono in cambiamenti nella forza delle connessioni sinaptiche tra i neuroni.) Così, la configurazione complessiva delle forze di connessione nella rete cambia a ogni ciclo operativo.

Per svolgere un particolare compito computazionale attraverso la rete, l'input (o gli input) del computo deve essere codificato come un insieme di segnali d'ingresso allo strato di input e il corrispondente segnale (o i corrispondenti segnali) di output deve essere interpretato come un risultato del calcolo. Il comportamento della rete - ciò che fa al segnale (o ai segnali) d'ingresso - dipende dal peso delle varie connessioni. In sostanza, lo schema di questi pesi costituisce la «memoria» della rete. La capacità di una rete neurale di svolgere un particolare compito in qualsiasi momento dipende dall'effettiva architettura della rete e dalla sua memoria in quel dato momento.

Allenare una rete neurale

Le reti neurali non sono programmate nel senso usuale di una programmazione di computer. Nella maggior parte dei casi, in particolare nelle reti neurali usate per compiere classificazioni, l'applicazione di una rete deve essere preceduta da un processo di «allenamento» per regolare i pesi delle varie connessioni.

A titolo di esempio, supponiamo che una banca voglia allenare una rete neurale a riconoscere usi non autorizzati di carte di credito. Per prima cosa la banca sottopone alla rete un gran numero di precedenti transazioni con carta di credito (registrate in termini di domicilio dell'utente, storia di accredito, tetto della carta, spesa, data, ammontare, luogo ecc.), per ognuna delle quali è noto se sia stata legittima o fraudolenta. Per ciascuna, la rete deve elaborare una previsione in merito alla legittimità della transazione. Se i pesi delle connessioni nella rete sono inizialmente

sistemati a caso o in qualche modo neutrale, allora alcune delle sue previsioni saranno corrette e altre sbagliate. Durante il processo di allenamento, la rete viene «premiata» ogni volta che la sua previsione è corretta e «punita» quando questa è sbagliata. (Ciò significa che la rete è costruita in modo che un «risultato corretto» - vale a dire, un feedback positivo per la sua previsione - fa sì che essa continui ad assestare i pesi delle connessioni come prima, laddove un «risultato sbagliato» la induce a regolarli in maniera differente.) Dopo molti cicli (migliaia o più), i pesi delle connessioni saranno regolati in modo tale che nella maggioranza dei casi (generalmente nella *grande* maggioranza) la decisione presa dalla rete risulta corretta. Quello che accade è che, dopo molti cicli di allenamento, i pesi delle connessioni nella rete si assesteranno in un modo che corrisponde ai profili dell'uso legittimo e fraudolento della carta di credito, qualunque essi siano (e, fatto molto importante, senza che il programmatore debba conoscerli).

Occorre molta abilità per tradurre queste idee generali in un sistema operativo, e sono state messe a punto molte architetture di rete differenti per costruire sistemi adatti a particolari compiti di classificazione.

Al termine di un riuscito ciclo di allenamento, è probabilmente impossibile per un operatore umano capire quali schemi o caratteristiche (per continuare col nostro esempio) delle transazioni con carte di credito la rete abbia imparato a identificare come indicatori di frode. Tutto ciò che l'operatore può sapere è che il sistema è accurato entro un certo margine di errore, dando una previsione corretta, poniamo, nel 95 per cento dei casi.

Un fenomeno simile può verificarsi anche con esseri umani particolarmente allenati ed esperti in un particolare ambito, come la medicina. Un medico esperto talvolta visiterà un paziente e dirà con una certa sicurezza che cosa crede non vada bene in lui, senza tuttavia essere in grado di spiegare esattamente quali sintomi specifici l'abbiano portato a trarre quella conclusione.

Gran parte del valore delle reti neurali proviene dal fatto che esse possono acquisire la capacità di discernere schemi di caratteristiche che nessun essere umano sarebbe in grado di scoprire. Per fare un esempio, generalmente solo una transazione con carta di credito su cinquantamila è fraudolenta. Nessun essere umano potrebbe monitorare un così gran numero di attività per identificare le frodi.

Di tanto in tanto, però, la stessa opacità delle reti neurali - il fatto che sono in grado di individuare schemi che un essere umano normalmente non riconoscerebbe come tali - può portare a risultati imprevisti. Secondo una storia che viene raccontata spesso, qualche anno fa l'esercito statunitense allenò una rete neurale a riconoscere delle cisterne nonostante fossero state dipinte con colori mimetici affinché si confondessero con lo sfondo. Il sistema fu allenato mostrandogli molte fotografie che rappresentavano scenari con e senza cisterne. Dopo svariati cicli di allenamento, la rete iniziò a esibire una capacità di riconoscimento delle cisterne estremamente accurata. Alla fine, arrivò il momento di provare il sistema sul campo, con vere cisterne situate in luoghi reali. E con sorpresa di tutti, il test diede risultati terribili: la rete sembrava fondamentalmente incapace di distinguere tra uno scenario con e uno senza cisterne. Gli ideatori del sistema, rossi di vergogna, si ritirarono in laboratorio sforzandosi di scoprire che cosa fosse andato storto. Alla fine, qualcuno capì qual era

stato il problema. Le fotografie utilizzate per allenare il sistema erano state scattate in due giorni diversi. Quelle con le cisterne erano state scattate in un giorno di sole, mentre quelle senza cisterne in una giornata nuvolosa. La rete neurale aveva indubbiamente appreso la differenza tra i due insiemi di fotografie, ma lo schema che aveva individuato non aveva nulla a che vedere con la presenza o assenza di cisterne; piuttosto, il sistema aveva imparato a distinguere uno scenario soleggiato da uno nuvoloso. La morale di questa storia è che, ovviamente, occorre stare attenti quando si intende stabilire quale sia esattamente lo schema che una rete neurale ha identificato. Ma, al di là di questa precauzione, le reti neurali si sono dimostrate estremamente utili in molti ambiti, dall'industria al commercio, dalla polizia alla difesa.

Sono state ideate varie architetture di rete per accelerare il processo di allenamento iniziale prima che una rete neurale possa essere messa all'opera, ma nella maggior parte dei casi tale processo impiega ancora un po' di tempo per essere completato. Le principali eccezioni sono le reti di Kohonen (dal nome del loro ideatore Tevo Kohonen), note anche con il nome di mappe autorganizzanti (SOM, *Self-Organizing Maps*), che vengono impiegate per identificare i raggruppamenti e che abbiamo già menzionato parlando del processo di raggruppamento dei crimini che sono probabilmente opera di un singolo individuo o di un'unica banda.

Le reti di Kohonen hanno un'architettura che incorpora una forma di misurazione della distanza, di modo che esse in sostanza allenano se stesse, senza il bisogno di un feedback esterno. Non avendo bisogno di un feedback, queste reti non richiedono nemmeno una gran quantità di dati precedenti; esse allenano se stesse compiendo cicli ripetuti attraverso i dati applicativi. Nondimeno, anche loro regolano i pesi delle connessioni, proprio come le altre reti neurali più frequentemente utilizzate.

Un vantaggio delle reti neurali sugli altri sistemi di *data mining* è che esse gestiscono molto meglio il problema dei dati mancanti che inevitabilmente si presenta con qualunque grande corpo di documentazioni raccolte dagli esseri umani.

Estrarre i dati sui crimini con le reti neurali

Sono stati messi a punto diversi sistemi commerciali per aiutare la polizia a risolvere, e qualche volta perfino a sventare, i delitti.

Un esempio è il Classification System for Serial Criminal Patterns (CSSCP), ideato dagli scienziati informatici Tom Muscarello e Kamal Dahbur alla DePaul University di Chicago. Il CSSCP passa al vaglio tutte le documentazioni di casi a sua disposizione, assegnando valori numerici a vari aspetti di ciascun crimine, come il tipo di reato, il sesso, l'altezza e l'età del colpevole, e il tipo di arma o di veicolo usato per la fuga. A partire da questi numeri esso costruisce un profilo descrittivo del crimine. Poi, una rete di Kohonen utilizza questo modello per cercare altri crimini con un profilo simile. Se trova un possibile collegamento tra due crimini, il CSSCP confronta i momenti e i luoghi in cui sono avvenuti per scoprire se gli stessi criminali avrebbero avuto abbastanza tempo per spostarsi da una scena del delitto all'altra. In una prova sperimentale del sistema, eseguita in laboratorio utilizzando i dati sulle

rapine a mano armata compiute nell'arco di tre anni, il sistema fu in grado di identificare un numero di schemi dieci volte superiore a quello individuato da una squadra di investigatori esperti che avevano accesso agli stessi dati.

Un altro programma di questo tipo è CATCH, che sta per Computer Aided Tracking and Characterization of Homicides. CATCH fu messo a punto dal Pacific Northwest National Laboratory per il National Institute of Justice e il Washington State Attorney General's Office. Il suo scopo è di aiutare gli agenti di polizia a determinare connessioni e relazioni tra i dati provenienti da indagini in corso e da casi risolti. CATCH fu costruito attorno al sistema di Homicide Investigation Tracking dello Stato di Washington, contenente i dati relativi a settemila omicidi e a seimila casi di aggressione sessuale nel Northwest. CATCH impiega una rete neurale di tipo kohoneniano per raggruppare i crimini in base a parametri come il modus operandi e le caratteristiche della firma dei delinquenti, consentendo agli analisti di confrontare un caso con casi simili registrati nella banca dati. Il sistema apprende informazioni circa un crimine passato, il luogo in cui è avvenuto e le sue caratteristiche peculiari. Il programma è suddiviso in differenti strumenti, ognuno dei quali pone l'enfasi su una certa caratteristica o gruppo di caratteristiche. Ciò consente all'utente di rimuovere le caratteristiche giudicate prive di collegamento.

Oggigiorno, un'attenzione particolare è rivolta al terrorismo. Secondo la storia di copertina apparsa su *Business Week* l'8 agosto 2005: «In base alle stime dell'FBI, dall'11 settembre in tutto il mondo sono stati arrestati più di tremila militanti di al Qaeda e sono stati fermati circa cento attacchi terroristici. I dettagli su come tutto ciò sia stato realizzato sono segretissimi. Ma senza dubbio due strumenti chiave sono stati lo spionaggio elettronico - mediante la rete segreta Echelon - e le tecniche informatiche di *data mining*».

Echelon è la rete globale di intercettazione gestita dalla National Security Agency (NSA) e dai suoi equivalenti in Canada, Gran Bretagna, Australia e Nuova Zelanda. I supercomputer della NSA passano al vaglio il flusso dei dati raccolti da Echelon per individuare indizi di macchinazioni terroristiche. I documenti che il sistema giudica meritevoli di attenzione passano nelle mani di traduttori e analisti umani, mentre il resto viene buttato via. Data la quantità di dati coinvolta, non sorprende che talvolta il sistema dia risultati migliori degli analisti umani, generando importanti informazioni troppo rapidamente perché gli esseri umani possano esaminarle. Ad esempio, due messaggi in arabo raccolti il 10 settembre 2001, che alludevano a un grande evento che sarebbe accaduto il giorno successivo, non furono tradotti fino al 12 settembre. (Dopo quel giorno, il più nero che si ricordi, fonti attendibili sostengono che il ritardo nelle traduzioni si è ridotto a circa dodici ore soltanto. L'obiettivo, naturalmente, è un'analisi condotta pressoché in tempo reale.)

Lo scopo ultimo è la creazione di sistemi di *data mining* in grado di esaminare accuratamente molteplici banche dati e di individuare correlazioni che avvertono di complotti in nuce. Il progetto di Terrorism Information Awareness (TIA) fu pensato per questo, ma il Congresso lo bocciò nel 2003 per preoccupazioni relative alla privacy. Oltre che per ispezionare banche dati commerciali e governative, il TIA fu progettato per creare esso stesso degli scenari terroristici - come un attacco al porto di New York - e poi determinare mezzi efficaci per scoprire e contenere i complotti. Ad

esempio, in quel caso avrebbe potuto esaminare le liste di clienti delle scuole di immersioni subacquee delle società che affittano le attrezzature necessarie, e poi cercare nomi simili nelle domande di visto e nelle liste dei passeggeri aerei.

Conosco quella faccia

I sistemi di riconoscimento facciale spesso fanno uso di reti neurali. Quelli attuali riducono il volto umano a una sequenza di numeri (talvolta chiamata «impronta facciale» o «vettore di caratteristiche»). Tali numeri sono le misurazioni di ottanta punti chiamati punti nodali (e delle loro reciproche distanze): caratteristiche fondamentali del volto come il centro degli occhi, la profondità delle orbite, gli zigomi, la linea della mandibola, il mento, la larghezza e la punta del naso (figura 3). Utilizzando computer veloci, è possibile calcolare l'impronta facciale di un individuo sospetto e confrontarla con le impronte facciali contenute in una banca dati nel giro di pochi secondi. Il confronto non può essere preciso, dal momento che l'angolo di osservazione dell'individuo in questione risulterà diverso da quello di ogni fotografia usata per generare l'impronta facciale nella banca dati, anche se questo effetto può essere in parte superato per mezzo di qualche calcolo trigonometrico elementare. Ma questo tipo di confronto, volto a individuare la «corrispondenza il più possibile esatta», è un compito che le reti neurali sono in grado di gestire bene.

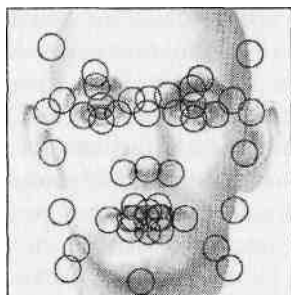


Figura 3. Diversi sistemi di riconoscimento facciale sono basati sulle misure di alcuni punti chiave del volto, chiamati punti nodali, e delle loro reciproche distanze.

Un vantaggio del confronto tra impronte facciali eseguito da una rete neurale è che questo non è influenzato da cambiamenti superficiali come il fatto di indossare o meno un cappello, di farsi crescere o tagliare la barba o gli effetti dell'età. Le prime organizzazioni a fare un ampio uso dei sistemi di riconoscimento facciale sono stati i casinò, che li utilizzavano per sorvegliare i giocatori con la fama di impostori. Il controllo dell'immigrazione negli aeroporti è un'applicazione più recente, e in rapida crescita, della medesima tecnologia.

Benché gli odierni sistemi di riconoscimento facciale non siano mai attendibili come quelli rappresentati nei film e negli spettacoli televisivi - soprattutto quando si tratta di riconoscere un volto nella folla, cosa che costituisce ancora una grossa sfida - la tecnologia risulta già utile in certe situazioni, e promette di diventare più accurata negli anni a venire. La ragione per cui il riconoscimento facciale è di qualche utilità nei casinò e negli uffici immigrazione aeroportuali è che in quei luoghi un individuo può essere fotografato da solo, a volto intero e su uno sfondo neutro. Ma persino in

questi casi si incontrano delle difficoltà. Ad esempio, nel 2005, la Germania iniziò a rilasciare passaporti biometrici, ma immediatamente si presentarono problemi dovuti al fatto che il sistema non funzionava se le persone sorridevano. Le autorità tedesche dovettero promulgare linee direttive che avvertivano che la persona doveva «avere un'espressione del volto neutra e guardare dritto nell'obiettivo della macchina fotografica».

D'altro canto, ci sono casi in cui il sistema ha dato risultati positivi. Il 25 dicembre 2004, il *Los Angeles Times* riferì di un fermo effettuato dalla polizia a ovest del centro di Los Angeles in cui i poliziotti, che stavano testando un nuovo sistema portatile di riconoscimento facciale, interrogarono una coppia di sospetti. Uno degli agenti puntò il sistema, un computer palmare con attaccata una macchina fotografica, verso uno dei due uomini. Il software di riconoscimento facciale contenuto nel dispositivo confrontò l'immagine con quelle di una banca dati che includeva foto di recenti evasi e di più di cento membri di due note bande di strada. Nel giro di qualche secondo, lo schermo esibì una sfilata di nove facce con profili simili a quello del sospetto. Il computer concluse che una di quelle immagini forniva la riproduzione più esatta delle caratteristiche del sospetto, con una probabilità di accuratezza del 94 per cento.

Il caso delle audioconferenze sospette

Individuare le frodi telefoniche è un'altra importante applicazione delle reti neurali.

Colleen McCue fu, per molti anni, addetta alla gestione dei programmi per l'unità di analisi del crimine presso il dipartimento di polizia di Richmond, in Virginia, dove fu una delle prime a fare uso delle tecniche di *data mining* nelle operazioni di polizia. Nel suo libro *Data Mining and Predictive Analysis*, ella descrive un progetto particolare a cui lavorò che illustra i molti passaggi che spesso occorre compiere per poter estrarre informazioni utili dai dati a disposizione. In questo caso una rete neurale di Kohonen fu impiegata per identificare raggruppamenti nei dati, ma, come spiega l'autrice, ci furono molti altri passaggi nell'analisi, che per la maggior parte dovettero essere compiuti manualmente. Proprio come, nelle ordinarie indagini di polizia, lo «sgobbare» della routine quotidiana e l'attenzione ai dettagli occupano molto più tempo che non le parti più affascinanti ed eccitanti messe in scena al cinema e in televisione, lo stesso accade con il *data mining*. In qualunque progetto, la laboriosa manipolazione e preparazione dei dati da parte degli esseri umani generalmente impiega una percentuale di tempo più elevata rispetto all'implementazione di sofisticati algoritmi matematici con strumenti ad alta tecnologia. (Questo, naturalmente, non significa che la matematica non sia importante; in realtà, è spesso di importanza cruciale. Ma di solito occorre molto lavoro preparatorio prima che la matematica possa essere applicata.)

Il caso descritto da McCue riguarda la creazione di un conto telefonico fraudolento che fu utilizzato per condurre una serie di conferenze telefoniche internazionali. Le indagini iniziarono quando una compagnia di servizi di conferenze telefoniche mandò

alla polizia una fattura di trentasette pagine con un elenco di audioconferenze effettuate senza pagare. Molte delle conferenze internazionali indicate sulla fattura erano durate tre ore o più. La compagnia aveva scoperto che le informazioni utilizzate per aprire il conto erano fraudolente. Le loro indagini li avevano portati a sospettare che le audioconferenze fossero state usate nel corso di un'attività criminale, ma non avevano nessun indizio concreto per identificare i colpevoli. McCue e i suoi colleghi si misero al lavoro per vedere se un'analisi di *data mining* delle audioconferenze potesse fornire qualche indizio sulla loro identità.

Il primo passo dell'analisi consistette nell'ottenere una copia elettronica del conto telefonico in un formato di testo facilmente processato. Grazie ai registri delle chiamate telefoniche, al giorno d'oggi ciò può essere realizzato piuttosto semplicemente ma, come confermeranno gli esperti di *data mining* in tutto il mondo, in molti altri casi all'inizio occorre investire una grande quantità di tempo e di energie nell'opera di reinserimento dei dati, così come nel controllo dei dati introdotti rispetto a quelli sullo stampato originale.

Il passo successivo fu di rimuovere dalla fattura tutte le informazioni non direttamente pertinenti per l'analisi, come le intestazioni, le informazioni sulle procedure di pagamento e così via. Il documento risultante includeva il codice di identificazione che il servizio di audioconferenze aveva rilasciato per ciascuna chiamata, i numeri telefonici dei partecipanti, le date e le durate delle telefonate. Meno del 5 per cento dei dati inseriti aveva il nome di un cliente, e anche se gli analisti li ritenevano falsi li conservarono comunque nell'eventualità potessero rivelarsi utili per collegamenti ulteriori.

Il documento fu quindi formattato in una forma strutturata suscettibile di analisi statistica. In particolare, i prefissi locali furono separati dalle altre informazioni, in quanto consentivano collegamenti basati sulle localizzazioni delle aree interessate, e allo stesso modo furono codificate separatamente le prime tre cifre dei numeri telefonici effettivi, essendo anch'esse collegabili a informazioni più specifiche riguardo alle località coinvolte. Le date furono rese più precise aggiungendo i giorni della settimana, per vedere se si riusciva a scorgere qualche schema regolare.

A quel punto, il documento conteneva 2017 chiamate. Tuttavia, un iniziale controllo visivo dei dati rivelò che in varie occasioni un singolo individuo aveva digitato il numero per entrare in una conferenza più di una volta. La maggior parte delle chiamate era di breve durata, meno di un minuto, e solo una era molto più lunga. La spiegazione più probabile era che gli individui interessati avessero difficoltà a connettersi a una conferenza o a mantenere la connessione. Di conseguenza, queste duplicazioni furono rimosse e rimase un totale di 1047 chiamate. I dati furono quindi sottoposti a una rete neurale di tipo kohoneniano. La rete rivelò tre raggruppamenti di telefonate simili, identificati sulla base del giorno del mese in cui la chiamata era stata effettuata e del numero di partecipanti coinvolti.

Ulteriori analisi delle telefonate nell'ambito dei tre raggruppamenti suggerirono la possibilità che le chiamate più brevi effettuate nei primi giorni del mese coinvolgessero soltanto i capi e che quelle alla fine del mese coinvolgessero l'intero gruppo. Sfortunatamente per la polizia (e per la compagnia telefonica i cui conti non furono pagati), attorno a quel periodo la banda aveva cessato la sua attività e non

c'era pertanto modo di portare avanti le indagini. Gli analisti ipotizzarono che questa cessazione improvvisa fosse premeditata, in quanto gli organizzatori della banda sapevano che al mancato pagamento del conto le autorità avrebbero avviato un'indagine.

Nessuno fu arrestato in quella occasione, ma le autorità ottennero una buona rappresentazione di come quel genere di attività criminali possano fare uso delle audioconferenze, ed è possibile che, basandosi sulle scoperte di quello studio, la compagnia telefonica abbia successivamente allenato una delle sue reti neurali a individuare schemi simili *nel momento in cui si presentano*, al fine di cogliere i colpevoli sul fatto. (Questo, naturalmente, è il genere di cose che le compagnie tendono a mantenere segrete.)

Battaglie come questa non finiscono mai. Le persone con intenti criminali continueranno a cercare modi per truffare le compagnie di telecomunicazioni. Il *data mining* è l'arma principale che queste ultime possiedono nel loro arsenale per fronteggiare i nemici che le minacciano.

Altri esempi di data mining in NUMB3RS

Dato l'ampio uso delle tecniche di *data mining* in molti ambiti della vita moderna, compresa l'individuazione e prevenzione del crimine, non sorprende che Charlie le menzioni in molti episodi di *NUMB3RS*. Ad esempio, nell'episodio *La rapina*, trasmesso in Italia il 29 luglio 2007, una serie a catena di furti in signorili case di Los Angeles prende una piega più inquietante quando uno dei padroni di casa viene ucciso. I ladri sembrano disporre di una considerevole quantità di informazioni circa gli oggetti di valore presenti nelle case che rapinano e sugli spostamenti dei padroni di casa. Eppure le case prese di mira sembrano non avere nulla in comune, e certamente nulla che indichi una fonte di quelle informazioni. Charlie utilizza un programma di *data mining* da lui ideato per cercare qualche regolarità tra tutti i furti avvenuti nella zona nel corso del periodo di sei mesi in cui si sono verificate le violazioni e, alla fine, scopre una serie di furti di automobili che potrebbe essere opera della stessa banda, il che porta alla cattura dei colpevoli.

Lettere consigliate

Jesus Mena, *Investigative Data Mining for Security and Criminal Detection*, Butterworth-Heinemann, Newton, MA, 2003.

Colleen McCue, *Data Mining and Predictive Analysis*, Butterworth-Heinemann, Newton, MA, 2007.

QUANDO È SUCCESSO?

Individuare i punti di cambiamento

Il genio dei numeri nel baseball

In un episodio della terza serie di *NUMB3RS*, trasmesso negli Stati Uniti con il titolo *Hardball*, un anziano giocatore di baseball, cercando di ritornare sulla scena dopo diversi anni bui nelle *minor leagues*, muore durante un allenamento sul campo. Quando l'allenatore apre l'armadietto del giocatore morto, trova una scorta segreta di aghi e di fiale di steroidi, e immediatamente contatta la polizia. Le indagini del coroner rivelano che il giocatore ha avuto un'emorragia cerebrale a causa di una massiccia overdose di steroidi, che aveva iniziato a usare per accrescere le sue prospettive di ritorno nella *major league*. Ma questa non è stata un'overdose accidentale. La droga trovata nel suo armadietto era trenta volte più potente del dosaggio normale, e doveva essere stata preparata appositamente. Il giocatore era stato ucciso.

Quando Don viene incaricato di risolvere il caso, scopre alcune e-mail sul computer portatile del giocatore, inviate da uno sconosciuto che sosteneva di sapere che egli stava assumendo sostanze dopanti e che lo minacciava di informare le autorità. Sembra trattarsi di un caso di estorsione. Ciò che è insolito è la prova che l'estorsore sosteneva di avere. Le e-mail recano un allegato, una pagina di formule matematiche che, in base a quanto affermava il mittente, mostravano esattamente in quale momento della sua carriera professionale il giocatore avesse iniziato ad assumere steroidi.

Chiaramente, questo era un altro caso in cui Don avrebbe avuto bisogno dell'aiuto di suo fratello. Charlie riconosce immediatamente di che tipo di matematica si tratti. «Questa è un'analisi statistica avanzata del baseball», sbotta.

«Esatto, *sabermetrica*», risponde Don, citando il termine tecnico che indica l'uso della statistica al fine di analizzare le prestazioni nel baseball.

Il termine «*sabermetrica*» deriva dall'acronimo SABR (Society for American Baseball Research) e fu coniato dal pioniere dell'analisi statistica del baseball Bill James, uno dei più entusiasti fautori dell'uso dei numeri per analizzare il gioco.

Charlie nota anche che chiunque abbia prodotto le formule ha ideato le proprie abbreviazioni matematiche, cosa che potrebbe aiutare a identificarne l'autore. Purtroppo, egli non conosce abbastanza la comunità degli studiosi di *sabermetrica* per avere un'idea di chi possa celarsi dietro alle e-mail. Ma un suo collega al CalSci riesce a fornire a Charlie le informazioni mancanti senza difficoltà. Una rapida ricerca di vari siti web dedicati al fantabaseball rivela presto messaggi inviati da un

individuo che fa uso delle stesse notazioni matematiche trovate nell'allegato delle e-mail ricattatorie.

Per Don, il quadro inizia ora a comporsi. Il giocatore era stato ucciso per evitare che parlasse dell'organizzazione che stava fornendo sostanze illegali a lui e molto probabilmente ad altri atleti. Ovviamente, le e-mail inviate dall'anonimo sabermetrico erano ciò che aveva suscitato il timore che l'organizzazione di narcotrafficienti venisse scoperta. Ma chi era l'assassino: la persona che aveva inviato le e-mail, il fornitore di droghe o qualcun altro?

Don non impiega molto tempo a risalire all'autore delle e-mail: Oswald Kittner, un venticinquenne fanatico di computer, che aveva abbandonato la scuola alle superiori e sfruttava le proprie abilità matematiche, acquisite da autodidatta, per condurre una bella vita vincendo soldi al fantabaseball. In questa arena virtuale, i giocatori creano ipotetiche squadre di giocatori reali, che giocano l'una contro l'altra in simulazioni al computer basate sulle statistiche correnti per i giocatori reali. Il successo di Kittner dipendeva dalle sue formule matematiche, che si dimostravano estremamente efficaci nell'identificare improvvisi cambiamenti nelle prestazioni di un giocatore: quella che negli ambienti della statistica viene chiamata «individuazione dei punti di cambiamento» (*change point detection*).

Come osserva Charlie, la ragione per cui il baseball si presta molto bene all'analisi statistica è la grande abbondanza di dati che genera circa le prestazioni individuali accoppiate con il ruolo del caso, cioè con il risultato altamente casuale che si ottiene a ogni tiro.

Ma Kittner aveva scoperto che la sua matematica poteva fare qualcos'altro oltre ad aiutarlo a fare soldi al fantabaseball. Essa permetteva di individuare quando un giocatore iniziava a fare uso di sostanze dopanti. Attraverso uno studio accurato delle prestazioni e dei comportamenti di noti utilizzatori di steroidi nel baseball, Kittner aveva determinato quali fossero i migliori dati statistici da considerare come indici dell'uso di steroidi: la quantità di palle lunghe battute, di giochi aggressivi (essere colpiti dai lanci, ad esempio) e anche di accessi d'ira (discussioni, espulsioni dal gioco e così via). Aveva quindi creato un sistema matematico di controllo per monitorare questi dati statistici per tutti i giocatori cui era interessato, di modo che se uno di loro avesse iniziato a fare uso di steroidi egli avrebbe individuato il cambiamento nei dati e avrebbe potuto agire rapidamente di conseguenza. Questo gli procurava informazioni attendibili circa il fatto che un certo giocatore stava facendo uso di steroidi molto prima che la cosa divenisse di pubblico dominio.

«E incredibile», esclama Charlie guardando di nuovo le formule. «Questo Kittner ha reinventato la procedura di Shirayev-Roberts per individuare i punti di cambiamento!»

Ma Kittner stava usando il suo metodo per ricattare i giocatori o semplicemente per vincere le partite di fantabaseball sapendo in anticipo che le prestazioni di un giocatore chiave stavano per migliorare drasticamente? Comunque sia, prima che il giovane tifoso potesse attuare il suo nuovo piano, uno dei suoi bersagli è stato ucciso. E ora questo genio della matematica e del computer si ritrova sospettato di omicidio.

Kittner presto confessa e inizia a collaborare con le autorità, e a Don non serve molto tempo per risolvere il caso.

Individuare i punti di cambiamento

Quando si ha a che fare con il crimine, prevenire è sempre meglio che cercare di catturare i colpevoli dopo il fatto. In certi casi, il vantaggio della prevenzione può essere molto più alto. Nel caso delle azioni terroristiche, come quelle dell'11 settembre 2001, l'unico modo per prevenire l'attacco è ottenere informazioni sui cospiratori prima che possano colpire. Questo è ciò che accadde nell'estate del 2006, quando le autorità britanniche prevennero un attacco multiplo su aerei transatlantici che doveva avvenire per mezzo di esplosivi liquidi portati a bordo camuffati da bibite e prodotti da toilette. Un attacco bioterroristico, d'altro canto, può impiegare settimane o mesi per giungere a pieno effetto, in quanto l'agente patogeno si fa strada lentamente attraverso la popolazione. Se le autorità fossero in grado di individuare l'agente patogeno in uno stadio relativamente precoce della sua diffusione, prima che l'effetto raggiunga proporzioni epidemiche, forse si potrebbe riuscire a contenerlo.

A tal fine, vari enti governativi hanno promosso i cosiddetti sistemi di *sorveglianza sindromica*, che prevedono la circolazione di liste di sintomatologie predefinite tra i membri del personale dei pronto soccorso ospedalieri e altri fornitori di cure mediche, i quali dovranno riferire alle agenzie di sanità pubblica la comparsa di tali sintomi. Queste agenzie monitorano i dati continuamente e impiegano analisi statistiche per determinare quando la frequenza di certi gruppi di sintomi è abbastanza superiore alla norma da giustificare il ricorso a certe azioni predefinite, tra cui, ad esempio, lanciare l'allarme. Alcuni dei più famosi sistemi attualmente operativi negli Stati Uniti sono RODS (Realtime Outbreak and Disease Surveillance) in Pennsylvania, ESSENCE (Early Notification of Community-Based Epidemics) a Washington, D.C., e il sistema BioSense implementato dai Centers for Disease Control and Prevention.

La principale sfida cui il creatore di un simile sistema di monitoraggio deve far fronte è identificare quando uno schema di attività - poniamo, un improvviso aumento del numero di persone che sul lavoro chiedono permessi per malattia o di persone che vanno dal medico mostrando determinati sintomi - indica qualcosa di insolito, sopra e oltre il normale flusso e riflusso di tali attività. Gli statistici chiamano questo lavoro «individuare un punto di cambiamento», ovvero stabilire che è avvenuto un determinato cambiamento, diverso dalle normali fluttuazioni.

Oltre che nella sorveglianza sindromica - avente lo scopo di accelerare la reazione a potenziali attacchi bioterroristici mediante la continua raccolta di dati medici quali i sintomi dei pazienti che si presentano nei pronto soccorso - gli algoritmi matematici per l'individuazione dei punti di cambiamento vengono usati per identificare altri tipi di attività criminali e terroristiche, come

- monitoraggio dei verbali della polizia per individuare aumenti nelle frequenze di certi crimini in determinate aree;
- ricerca delle variazioni negli andamenti delle transazioni finanziarie che potrebbero indicare un'attività criminale.

Nati nel mondo dell'industria

Il primo impiego significativo dei sistemi di individuazione dei punti di cambiamento, tuttavia, non fu per combattere il crimine, ma per migliorare la qualità dei prodotti industriali. Nel 1931 Walter A. Shewhart pubblicò un libro che spiegava come monitorare i processi di produzione tenendo traccia dei dati in un diagramma di controllo.

Shewhart, nato nel 1891 a New Canton nell'Illinois, aveva studiato fisica alle università dell'Illinois e della California, conseguendo alla fine un dottorato di ricerca, ed era stato professore universitario per qualche anno prima di andare a lavorare per la Western Electric Company, che produceva apparecchiature per la Bell Telephone. Nei primi tempi dell'industria telefonica il malfunzionamento delle apparecchiature era un grosso problema, e tutti si resero conto che la chiave del successo era di migliorare il processo di produzione. Ciò che Shewhart fece fu dimostrare come un uso intelligente della statistica potesse aiutare a risolvere il problema.

La sua idea era di monitorare un'attività, come una linea di produzione, e cercare un cambiamento. La parte difficile era decidere se un rilevamento insolito costituiva solo un'anomalia - una delle tante fluttuazioni casuali che frequentemente si incontrano nel mondo - oppure un segno che qualcosa era cambiato (un punto di cambiamento, figura 4).

Chiaramente, occorre osservare qualche rilevamento ulteriore prima di conoscere la risposta. Ma quanti altri rilevamenti? E quanto possiamo essere sicuri che ci sia stato davvero un cambiamento e non solo una sfortunata, ma in ultima analisi insignificante, serie di rilevamenti inattesi? Qui occorre cercare un punto d'equilibrio. Maggiore è il numero di rilevamenti ulteriori, più si può essere certi che c'è stato un cambiamento, ma bisognerà attendere più a lungo prima di poter prendere qualche provvedimento. Shewhart suggerì un metodo semplice ma funzionale: aspettare semplicemente fino a che non si osserva un risultato insolito statisticamente molto lontano dalla media, poniamo di tre deviazioni dallo standard. Questo metodo rappresentò un enorme progresso, ma poteva volerci ancora molto tempo prima che un cambiamento venisse individuato: un tempo troppo lungo per molte applicazioni, in particolare per quelle coinvolte nella scoperta delle attività criminali e nella prevenzione degli attacchi terroristici. Per un vero progresso la chiave era usare la matematica.

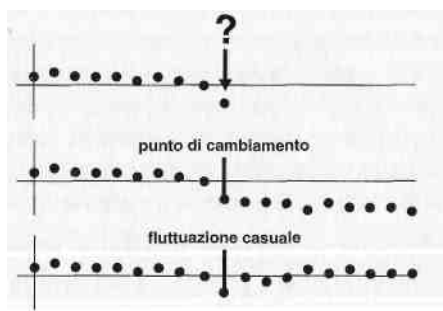


Figura 4. Un dato anomalo è solo una fluttuazione casuale o è indice di un cambiamento?

Entra in scena la matematica

Circa venticinque anni dopo la comparsa del libro di Shewhart alcuni matematici, E.S. Page in Inghilterra, A.N. Shiryayev in Unione Sovietica e S.W. Roberts negli Stati Uniti, trovarono diversi modi molto più efficienti (e matematicamente sofisticati) per individuare i punti di cambiamento.

Con il fiorire della teoria matematica, maturò anche la comprensione nell'industria e in vari ambiti del governo (compresi quelli della polizia) del fatto che i metodi di individuazione dei punti di cambiamento potevano essere applicati a un'ampia gamma di problemi del mondo reale. Oggi si sa che tali metodi risultano utili non solo nel controllo della qualità dei prodotti industriali ma anche in aree come:

- il monitoraggio medico;
- le applicazioni militari (ad esempio, il monitoraggio dei canali di comunicazione);
- la protezione dell'ambiente;
- i sistemi elettronici di sorveglianza;
- la sorveglianza di sospette attività criminali;
- il monitoraggio della sanità pubblica (ad esempio, la difesa dal bioterrorismo);
- il controterrorismo.

Per mostrare come funziona un metodo di individuazione dei punti di cambiamento più efficiente, ci concentreremo sulla procedura di Page. (Il metodo di Shiryayev-Roberts menzionato da Charlie Eppes è leggermente più tecnico da descrivere.) Considereremo un esempio più semplice del controllo di qualità: nella fattispecie, l'individuazione di un aumento nella frequenza di qualche evento.

Supponiamo che nel corso di qualche sostanziale periodo di tempo si sia osservato che un particolare evento si verifica circa una volta al mese. In altre parole, la probabilità che esso accada in un giorno qualunque è uno su trenta. Gli esempi abbondano: una newyorkese che trova parcheggio nella via di fronte al suo appartamento, un marito che *si offre* di portar fuori la spazzatura, un notiziario televisivo locale che non si apre con un caso di catastrofe naturale o di crimine violento e così via.

Supponiamo ora che la frequenza di un dato evento possa aumentare drasticamente, poniamo a una volta la settimana. Vogliamo predisporre un sistema di individuazione dei punti di cambiamento che sia in grado di reagire il più rapidamente possibile senza lanciare un falso allarme troppo spesso.

Il problema fondamentale con cui dobbiamo fare i conti è che fluttuazioni casuali come tre o quattro occorrenze dell'evento in un unico mese possono dare l'impressione che la frequenza sia cambiata da una volta ogni trenta giorni a una volta ogni sette giorni, anche quando in realtà non c'è stato un vero cambiamento.

Nella procedura di Page, introduciamo un indice matematico, S , che traccia l'attività. Il valore di S è fissato inizialmente a 1 e viene corretto ogni giorno utilizzando determinati calcoli di probabilità, come vedremo brevemente. Quando il

valore di S raggiunge o supera un certo livello prefissato (diciamo 50 nel nostro esempio), possiamo dichiarare che è avvenuto un cambiamento. (Si noti che *non* occorre stimare *quando* esattamente il cambiamento sia avvenuto, ma solo stabilire se è avvenuto o meno.)

Come si fa ad «aggiornare» S ogni giorno? Si moltiplica S per la probabilità di qualunque cosa sia accaduta quel giorno, *ipotizzando che si sia già verificato un cambiamento*, e si divide il risultato per la probabilità di qualunque cosa sia accaduta, *ipotizzando che non si sia ancora verificato un cambiamento*.

Nel nostro esempio, ciò significa che se l'evento si verifica, moltiplichiamo S per $1/7$ e dividiamo il risultato per $1/30$ (cioè moltiplichiamo per 4,286); mentre se l'evento non si verifica, moltiplichiamo S per $6/7$ e dividiamo il risultato per $29/30$ (cioè moltiplichiamo per 0,8867). Nel primo caso, il valore di S aumenterà. Nel secondo caso, S diminuirà; se il nuovo valore di S è inferiore a 1, riportiamo S a 1. (Non lasciando mai che S abbia un valore inferiore a 1, il processo rimane pronto a reagire a un cambiamento in qualunque momento.)

Poiché l'evento cui siamo interessati è *più probabile una volta che sia avvenuto un cambiamento*, nei giorni in cui esso accade S diventa più grande. E, naturalmente, S diventa più piccolo nei giorni in cui l'evento non si verifica.

Tale procedura è facile da eseguire con una calcolatrice. Supponiamo di iniziare da zero e di osservare quanto segue nei giorni successivi:

No, No, Sì (l'evento è accaduto), No, No, No, No, No, No, Sì,...

Iniziamo con $S = 1$. Il primo «No» dà $S = 1 \times 0,8867 = 0,8867$, pertanto ripristiniamo $S = 1$. Anche il secondo «No» dà $S = 0,8867$ e di nuovo riportiamo S a 1. Poi abbiamo un «Sì», così che S diventa $1 \times 4,286 = 4,286$. Il successivo «No» dà $S = 4,286 \times 0,8867 = 3,800$.

Procedendo lungo la sequenza di osservazioni, otteniamo in successione i valori 3,370; 2,988; 2,649; 2,349; 2,083; e a quel punto incontriamo il secondo «Sì», che dà $S = 8,927$.

Se continuiamo a ottenere «Sì» così spesso, S raggiungerà una soglia come 50 piuttosto rapidamente. Ma anche *dopo* che è avvenuto un cambiamento a una probabilità di uno su sette ogni giorno, non è infrequente che passino due settimane senza che l'evento si verifichi, e ciò moltiplicherebbe S per 0,8867 ogni giorno, a meno che non entri in gioco la regola di «non lasciare mai che S sia inferiore a 1».

Se utilizziamo un computer per generare giorni casuali con una probabilità di uno su trenta che l'evento accada ogni giorno, e ogni giorno è una nuova prova, indipendente dalla storia passata, risulta che quando per S viene usata una soglia di 50, falsi indicatori di cambiamento si presenteranno all'incirca ogni 1250 giorni, vale a dire più o meno ogni tre anni e mezzo. D'altro canto, il tempo che può passare prima che venga individuato un cambiamento a una probabilità di uno su sette ogni giorno è in media non più di trentatré giorni - circa un mese - anche se il cambiamento avviene quando capita che S sia uguale a 1 (il più basso valore possibile), come all'inizio del processo. Questo è molto meglio di ciò che era in grado di fare la procedura di Shewhart.

Con il metodo di Page, possiamo ottenere un vasto intervallo tra i falsi indicatori (noto agli statistici come lunghezza media delle sequenze o ARL, da *average run length*) pagando un prezzo limitato in termini di aumento del tempo necessario per individuare un cambiamento. Grandi aumenti della ARL sono accompagnati da incrementi piuttosto piccoli nel tempo di scoperta. La tabella 5 mostra alcuni risultati (per questo esempio) che illustrano il compromesso.

Soglia	ARL	Tempo di scoperta
18,8	1,3 anni	25,2 giorni
40	2,5 anni	30,3 giorni
50	3,4 anni	32,6 giorni
75	5,2 anni	36,9 giorni
150	10,3 anni	43,8 giorni

Tabella 5. Rapporto tra ARL e tempo di scoperta.

Ma, pur costituendo un grosso miglioramento rispetto al metodo di Shewhart, la procedura di Page sembra richiedere ancora molto tempo per individuare un cambiamento in maniera attendibile. Possiamo fare di meglio? Sfortunatamente esistono limiti teorici ai risultati che si possono raggiungere, come dimostrò nel 1986 un matematico di nome G.V. Moustakides. I suoi studi confermarono che quando le distribuzioni dei valori dei dati prima e dopo un possibile cambiamento sono noti, come nel nostro esempio, la procedura di Page è il meglio che si possa fare.

Questo limite fondamentale alla capacità di individuare in maniera attendibile i punti di cambiamento non è solo frustrante per gli statistici, ma lascia la società irrimediabilmente vulnerabile alle minacce in aree come il bioterrorismo.

Scoprire in tempo un attacco bioterroristico

Un buon esempio in cui l'individuazione dei punti di cambiamento risulta cruciale è la *sorveglianza sindromica*, cui abbiamo accennato all'inizio del capitolo. L'idea fondamentale, che viene attualmente applicata da molti dipartimenti di sanità statali e locali in tutti gli Stati Uniti, in collaborazione con alcuni enti del governo federale, è la seguente: supponiamo che un attacco terroristico impieghi un agente come l'antrace o il vaiolo che può essere rilasciato senza provocare un allarme immediato, di modo che la malattia riesce a diffondersi per qualche tempo senza insospettire gli ospedali e i funzionari della sanità pubblica.

Nel caso di un simile attacco è di importanza fondamentale che l'allarme giunga alle autorità, in particolare nell'ambito del sistema di sanità pubblica, il più presto possibile affinché possano rendersi conto di ciò che sta accadendo e adottare contromisure appropriate. Queste potrebbero includere avvisi pubblici e comunicati a medici e ospedali che descrivono quali sintomi cercare nei pazienti, quante persone sono state probabilmente colpite e in quali aree, e quali metodi usare nella diagnosi e

nella cura.

In assenza di qualche sistema capace di accelerare la reazione delle autorità, potrebbero facilmente verificarsi ritardi sostanziali. L'esecuzione di test medici e la conferma delle diagnosi possono richiedere un po' di tempo, e l'eventualità che i primi pazienti siano pochi e sparsi contribuirebbe alla difficoltà di riconoscere una crescente minaccia.

Scontrandosi con i limiti implicati dai risultati di Moustakides del 1986, i ricercatori nel campo dell'individuazione dei punti di cambiamento sono costantemente in cerca di migliori fonti di dati per raggiungere l'obiettivo ultimo: la scoperta il più possibile precoce di un cambiamento.

Nell'ottobre del 2006 si tenne a Baltimora, nel Maryland, la quinta conferenza annuale sulla sorveglianza sindromica. Gli articoli di ricerca presentati alla conferenza coprivano argomenti come: migliorare la tempestività della scoperta attraverso modelli corretti in base ai ritardi nella disponibilità dei dati; il potere di previsione sindromica: confrontare covariate e dati di partenza; simulazione efficiente su larga scala delle epidemie basata su reti; procedure operative standard per tre sistemi di sorveglianza sindromica nella contea di Washoe, in Nevada.

Maggiore è la variabilità naturale, più serio è il problema dei falsi allarmi. Ma esiste un altro fattore aggravante: la stessa molteplicità dei sistemi di sorveglianza. I ricercatori che parteciparono alla conferenza fecero notare che nel prossimo futuro potrebbero esserci migliaia di tali sistemi operanti simultaneamente per tutti gli Stati Uniti. Anche se la frequenza dei falsi allarmi è ben controllata in ogni sistema, il loro tasso complessivo sarà migliaia di volte maggiore, portando a costi e a problemi evidenti, compreso il classico fenomeno del «ragazzo che gridava 'al lupo'»: troppi falsi allarmi desensibilizzano le persone nei confronti degli eventi reali.

Come possiamo affrontare i problemi di carattere medico e politico e le sfide matematiche associate alla sorveglianza sindromica?

In molti studi recenti, i ricercatori hanno impiegato simulazioni al computer per stimare l'efficacia dei differenti metodi matematici quando vengono applicati a casi reali. I risultati mostrano in maniera coerente che se si confrontano gli approcci di Shewhart e di Page, il secondo si rivela migliore. Questa non è una conclusione scontata, dal momento che il teorema di Moustakides, che afferma che la procedura di Page è la migliore possibile, non si applica alla lettera ai complessi problemi che i ricercatori stavano cercando di risolvere. Ma i matematici sono avvezzi al fenomeno, per cui quando è stato dimostrato che un metodo o un algoritmo è il migliore possibile in qualche semplice situazione è probabile che si dimostri tale anche in situazioni più complesse.

I ricercatori si stanno dando molto da fare per migliorare l'efficacia dei sistemi di sorveglianza sindromica. Gli scenari antecedenti al cambiamento richiedono una conoscenza accurata dei dati di partenza: vale a dire, la comparsa nel pronto soccorso di pazienti che presentano una determinata combinazione di sintomi. Gli esperti fanno anche molta attenzione al miglioramento delle stime di probabilità che vanno nella parte dei calcoli corrispondente a «prima del cambiamento». Molti dei più comuni insiemi di sintomi ricercati da questi sistemi di sorveglianza hanno una maggiore probabilità di falsi positivi in certi periodi dell'anno - ad esempio in quelli

con una più alta incidenza di raffreddori e influenze - così che i calcoli risultano molto più accurati quando le probabilità di partenza sono definite in un modo che riflette gli effetti stagionali.

Un'altra chiave per migliorare questi sistemi è affinare le stime delle probabilità per gli scenari successivi al cambiamento (postattacco). Uno studio recente esamina la possibilità di migliorare la biosorveglianza incorporando informazioni geografiche nell'analisi. Creando misure statistiche del modo in cui si raggruppano le segnalazioni dei sintomi - in particolare la loro distribuzione spaziale e temporale - i sistemi di sorveglianza potrebbero migliorare la loro capacità di individuare epidemie o andamenti anomali nell'incidenza di una malattia.

I matematici dispongono di qualche altro asso nella manica che potrebbe rivelarsi utile. I metodi della statistica bayesiana (di cui parleremo nel capitolo 6) possono essere utilizzati per incorporare certi tipi di informazioni utili nei calcoli per l'individuazione dei punti di cambiamento. Supponiamo che mentre stiamo monitorando un flusso di dati, alla ricerca di un punto di cambiamento, qualcuno ci dia qualche suggerimento, sussurrandoci all'orecchio in quali punti è più o meno probabile che avvenga un cambiamento. Questo è più o meno ciò che fa il sistema di allarmi pubblici a colori del dipartimento della Sicurezza interna degli Stati Uniti, e le informazioni raccolte e valutate dai servizi segreti possono essere utilizzate per fornire allarmi più specifici per certi tipi di attacchi bioterroristici. I metodi bayesiani possono incorporare tali informazioni in maniera molto naturale e sistematica: di fatto, abbassando la soglia per lanciare un allarme nei periodi in cui le probabilità di certi tipi di attacchi bioterroristici sono più elevate.

Riassumendo la situazione attuale nella sorveglianza sindromica, un matematico ha recentemente affermato: «L'individuazione dei punti di cambiamento è morta. O meglio, lunga vita all'individuazione dei punti di cambiamento».

MIGLIORARE E RICOSTRUIRE LE IMMAGINI

Il pestaggio di Reginald Denny

Il 29 aprile 1992, alle 17.39, Reginald Oliver Denny, un camionista bianco di trentanove anni, caricò ventisette tonnellate di sabbia sul suo autocarro rosso a diciotto ruote e partì per consegnarle a uno stabilimento di Inglewood, in California. Non aveva la minima idea del fatto che, poco più di un'ora dopo, milioni di telespettatori lo avrebbero visto mentre veniva ridotto quasi in fin di vita dalle percosse di una banda di rivoltosi. E nemmeno si poteva aspettare che il conseguente processo penale contro i suoi aggressori avrebbe coinvolto un'applicazione davvero notevole della matematica.

La sequenza di eventi che portò al pestaggio di Denny era iniziata un anno prima, il 3 marzo 1991, quando gli agenti della pattuglia autostradale della California videro un giovane maschio nero di ventisei anni, Rodney Glenn King, guidare ad alta velocità sull'autostrada interstatale 210. I poliziotti inseguirono King per tredici chilometri a una velocità di 160 chilometri orari, prima di riuscire alla fine a fermarlo a Lake View Terrace. Quando gli agenti della pattuglia gli ordinarono di mettersi a terra, King si rifiutò. A quel punto, giunse sulla scena una volante con quattro agenti del dipartimento di polizia di Los Angeles, e il sergente Stacey Koon prese il comando della situazione. Quando King si rifiutò nuovamente di obbedire all'ordine di mettersi a terra, il sergente Koon ordinò ai suoi agenti di usare la forza. I poliziotti iniziarono quindi a colpire King con i manganelli, e continuarono a bastonarlo a lungo anche dopo che era caduto a terra. Quello che i poliziotti non sapevano era che uno spettatore, George Holliday, stava registrando con una telecamera tutta la scena e che successivamente avrebbe venduto la registrazione alle reti televisive.

In gran parte sulla base delle videoregistrazioni, che furono viste da telespettatori di tutto il mondo, i quattro agenti, tre bianchi e un latinoamericano, furono accusati di «aggressione con la forza capace di produrre gravi ferite fisiche» e di aggressione «sotto il pretesto dell'autorità». Come l'avvocato difensore dei poliziotti argomentò in tribunale, il video mostrava che King si era comportato in maniera barbara e violenta per tutto il corso della vicenda (fu alla fine accusato di resistenza a pubblico ufficiale, anche se l'accusa fu successivamente ritirata), ma come risultato del notevole interesse che la videoregistrazione di Holliday aveva suscitato, il centro dell'attenzione non era più King, bensì le azioni dei poliziotti. Il caso giudiziario si svolse sullo sfondo esplosivo di una città in cui le tensioni razziali erano alte e i rapporti tra la comunità nera e gli agenti di polizia, per lo più bianchi, erano assai burrascosi. Quando, il 29 aprile 1992, tre degli agenti furono assolti da una giuria composta da dieci membri bianchi, uno latinoamericano e uno asiatico (la giuria non riuscì a venire a un accordo sul verdetto per uno dei capi d'accusa contro uno degli

imputati) , grandi rivolte esplosero in tutta la regione di Los Angeles.⁹

Le sommosse durarono tre giorni, dando vita a uno dei peggiori disordini civili nella storia di Los Angeles. Prima che la polizia, i marines e la guardia nazionale ristabilissero l'ordine, ci furono 58 morti, 2383 feriti, più di 7000 interventi antincendio e danni a circa 3100 negozi per un valore di oltre un miliardo di dollari. Rivolte razziali minori esplosero anche in altre città americane. Il primo maggio 1992, il terzo giorno delle sommosse di Los Angeles, Rodney King andò in televisione per lanciare un appello che invitava alla calma e alla pace, chiedendo: «Gente, voglio solo dire, riusciamo ad andare tutti d'accordo?»

Ma i tumulti erano scoppiati soltanto da poche ore quando il camionista Reginald Denny uscì dall'autostrada di Santa Monica e prese una scorciatoia attraverso Florence Avenue. Alle 18.46, dopo aver imboccato l'incrocio con Normandie Avenue, si ritrovò circondato da rivoltosi neri che iniziarono a gettargli pietre contro i finestrini e sentì qualcuno che gli gridava di fermarsi. Dall'alto, un elicottero pilotato dal cronista Bob Tur filmò la seguente scena.

Un uomo aprì la portiera del camion e gli altri trascinarono Denny fuori. La vittima fu gettata a terra e uno degli aggressori gli tenne giù la testa col piede. Denny, che non aveva fatto nulla per provocare l'aggressione, fu colpito con un calcio allo stomaco. Qualcuno gli lanciò un pesante attrezzo medico in testa e lo colpì tre volte con un martello da falegname. Un altro uomo ancora gli gettò una piastra di calcestruzzo in testa facendogli perdere coscienza. L'uomo, che come si scoprì in seguito rispondeva al nome di Damian Williams, fece quindi una danza della vittoria, mostrando il simbolo di una banda all'elicottero che volava a punto fisso sopra di loro e che stava trasmettendo la scena in diretta, e puntò il dito verso Denny. Un altro rivoltoso poi sputò addosso a Denny e se ne andò assieme a Williams. Diversi passanti fotografarono la scena ma nessuno andò a soccorrere la vittima.

Quando il pestaggio ebbe fine, vari uomini gettarono bottiglie di birra contro il corpo incosciente di Denny. Qualcuno si avvicinò a lui e rovistò nelle sue tasche rubandogli il portafogli. Un altro uomo si fermò vicino al corpo e tentò di sparare al serbatoio del camion ma fallì il colpo. Alla fine, quando gli aggressori se n'erano andati, quattro uomini che avevano visto la scena in televisione andarono a soccorrere Denny. Uno di loro era un camionista e poteva quindi guidare il mezzo di Denny. Così i quattro soccorritori caricarono il corpo massacrato della vittima nella cabina del suo autocarro e lo portarono all'ospedale. Poco prima di arrivare in ospedale, Denny ebbe un attacco epilettico.

I paramedici che si occuparono di lui dissero che era arrivato molto vicino alla morte. Aveva il cranio fratturato in novantun punti e infossato fino a ledere il cervello. Il suo occhio sinistro era talmente fuori posto che sarebbe caduto nella cavità sinusale se i chirurghi non avessero sostituito l'osso frantumato con un pezzo di plastica. Tuttora nella sua testa rimane un cratere, nonostante gli sforzi per correggerlo.

Il notiziario video registrato dall'elicottero di Bob Tur consentì di identificare i tre uomini più direttamente coinvolti nell'aggressione di Denny, i quali furono arrestati e

⁹ Dopo le rivolte, contro i quattro poliziotti furono mosse accuse federali di violazione dei diritti civili. Il sergente Stacey Koon e l'agente Laurence Powell furono giudicati colpevoli, mentre gli altri due furono assolti.

portati in giudizio. Dei tre solo uno, Damian Williams, fu giudicato colpevole, e soltanto di uno dei capi d'accusa, in quanto la corte parve essere dell'idea (a torto o a ragione) che le azioni non fossero premeditate ma fossero il risultato della mentalità rivolta che aveva permeato l'intera città. Per il nostro scopo presente, tuttavia, l'aspetto più affascinante del caso è che l'identificazione di Williams dipese dall'applicazione di alcune nuove tecniche matematiche importanti e che la loro accettazione da parte della corte segnò un momento epocale nella storia giuridica.

Il tatuaggio della rosa

Sebbene milioni di persone avessero visto l'aggressione di Denny in televisione, sia in diretta sia nel corso delle infinite repliche che furono trasmesse nei programmi di attualità, e sebbene nel processo contro Williams e i suoi due complici gli avvocati dell'accusa avessero mostrato quaranta minuti di videoregistrazioni dell'evento come prova, si dimostrò difficile identificare gli aggressori in maniera sufficientemente attendibile da ottenere una condanna. Il filmato era stato ripreso con una piccola telecamera portatile, manovrata dalla moglie di Tur, Marika, in un elicottero in volo a punto fisso sopra la scena. Le immagini risultanti erano sgranate e sfocate, e in nessuna occasione Marika Tur era riuscita a ottenere una chiara inquadratura dei volti degli aggressori. L'uomo che nel filmato si vedeva lanciare una grande piastra di calcestruzzo contro la testa di Denny e poi esibirsi in una danza della vittoria sul corpo incosciente della vittima *poteva* essere Williams. Ma poteva anche essere uno qualunque delle centinaia di giovani neri nell'area di Los Angeles con una corporatura e un aspetto molto simili ai suoi.

Una caratteristica che distingueva Williams da altri possibili sospetti era una grossa rosa tatuata sul suo braccio sinistro. (Il tatuaggio lo identificava come un membro di una nota banda di Los Angeles chiamata Eight Tray Gangster Crips.) Sfortunatamente, anche se alcuni fotogrammi del notiziario video mostravano il braccio sinistro dell'aggressore, l'immagine non era abbastanza nitida per distinguere il tatuaggio.

Ma dopo alcuni momenti di frustrazione iniziale, gli avvocati dell'accusa ebbero un colpo di fortuna. Un cronista di Santa Monica fornì loro alcune fotografie scattate da un elicottero con un obiettivo a lunga distanza di 400 millimetri. Queste fotografie avevano una risoluzione molto più alta delle immagini del filmato e un esame attento di una di esse, sia a occhio nudo sia con la lente d'ingrandimento, rivelò una confusa regione grigia sul braccio sinistro dell'aggressore mentre stava in piedi sopra il corpo disteso di Denny (figura 5). In effetti, la regione grigia - appena un seimillesimo dell'area complessiva della fotografia - poteva essere un tatuaggio, ma poteva anche essere una macchia di sporco oppure un'imperfezione della fotografia. E qui che entrò in scena la matematica.

Utilizzando tecniche matematiche molto sofisticate, messe a punto originariamente per migliorare le fotografie di controllo scattate

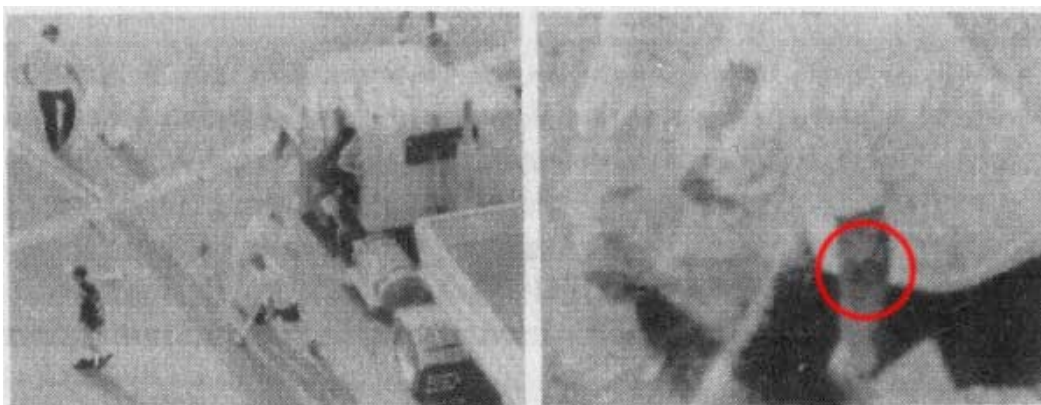


Figura 5. Fotografia aerea dell'aggressione subita da Reginald Denny: nel particolare, ingrandito tramite sofisticate tecniche matematiche, si può notare il tatuaggio sul braccio dell'aggressore.

dai satelliti militari, la porzione cruciale della fotografia fu elaborata su un computer per generare un'immagine molto più chiara. L'immagine risultante rivelò che l'apparente segno sul braccio sinistro dell'aggressore, al di là della consueta soglia legale «di ogni ragionevole dubbio», aveva la stessa forma e lo stesso colore della rosa tatuata sul braccio di Damian Williams.

Le tecniche impiegate per elaborare le immagini fotografiche nel caso di Reginald Denny cadono nell'area generale nota come *ottimizzazione delle immagini*. Non si tratta di tecniche per aggiustare la luminosità, il colore o il contrasto, o per rifinire le fotografie in qualche altro modo, come quelle note agli utenti di computer nella forma di programmi quali Photoshop, né dei software proprietari di gestione delle fotografie che vengono spesso dati in dotazione con le nuove macchine fotografiche digitali. Nell'ambito dell'ottimizzazione delle immagini, vengono utilizzate tecniche matematiche per *ricostruire* dettagli di un'immagine deteriorati dalla sfocatura nella fotografia originale.

Il termine «ricostruire» come viene usato qui può essere fuorviante per un profano che non abbia familiarità con la tecnica. Per gli esperti che elaborarono le immagini nel processo contro Damian Williams uno dei passaggi chiave fu di convincere il giudice, e quindi la giuria, che la procedura era affidabile e che l'immagine risultante non mostrava «ciò che *avrebbe potuto* essere» ma rivelava effettivamente «quello che *era*». La deliberazione del giudice in quel caso, che le immagini prodotte dalle tecniche di ottimizzazione costituivano prove accettabili, rappresentò una svolta epocale nella storia giuridica.

L'idea generale dietro le tecniche di ottimizzazione è di usare la matematica per fornire caratteristiche dell'immagine non catturate nella fotografia originale. Nessuna fotografia è in grado di rappresentare tutti gli elementi di una scena visiva. La maggior parte delle fotografie cattura una quantità di informazioni tale da far sì che l'occhio umano sia spesso incapace di cogliere qualche differenza tra la fotografia e la scena originale, e certamente sufficiente per permetterci di identificare una persona. Ma, come hanno dimostrato gli scienziati cognitivi, molto di quello che vediamo quando guardiamo una scena reale o una fotografia è un prodotto del nostro cervello, il quale riempie - generalmente in modo affidabile e accurato - qualunque cosa che (per una ragione o per l'altra) manchi nel segnale visivo effettivamente percepito dai nostri occhi. Quando si tratta di certe particolari caratteristiche di

un'immagine, la matematica è molto più potente e può fornire - anch'essa in modo affidabile e accurato - dettagli che la fotografia in origine non è riuscita a catturare pienamente.

Nel processo contro Damian Williams, il principale testimone dell'accusa che identificò l'imputato fu Leonid Rudin, cofondatore nel 1988 della Cognitech Inc., una compagnia di Santa Monica specializzata nell'elaborazione di immagini. Quando era uno studente di dottorato al California Institute of Technology a metà degli anni '80, Rudin aveva ideato un nuovo metodo per eliminare la sfocatura delle immagini fotografiche. Lavorando con i suoi colleghi alla Cognitech, egli aveva sviluppato ulteriormente la tecnica al punto che, quando Damian Williams fu portato in giudizio, la sua squadra poté prendere le immagini video del pestaggio ed elaborarle matematicamente per produrre un fermo immagine che mostrava che ciò che nel video originale sembrava una macchia a malapena discernibile sull'avambraccio di uno degli aggressori era chiaramente identificabile come un tatuaggio simile a quello presente sul braccio di Williams. Quando la fotografia ricostruita fu presentata alla giuria per l'identificazione, i difensori di Williams immediatamente modificarono la loro posizione da «Williams non è la persona nella fotografia/video» a «le sue azioni non erano premeditate».

Quello che l'occhio non può vedere: la matematica della ricostruzione di immagini

Per farci un'idea del tipo di problema con cui gli ingegneri della Cognitech dovettero misurarsi, immaginiamo di dover affrontare il compito, a confronto più semplice, di ingrandire una fotografia (o parte di una fotografia) fino al doppio della sua dimensione originaria. (L'ingrandimento della parte fondamentale dell'immagine di Williams fu in effetti una delle cose che Rudin e i suoi colleghi fecero come parte della loro analisi.) Il modo più semplice è di aggiungere più pixel in base a qualche semplice regola. Ad esempio, supponiamo di iniziare con un'immagine memorizzata come una griglia di 650 x 500 pixel e di voler generare una versione ingrandita che misuri 1300 x 1000 pixel. Il primo passo consiste nel raddoppiare le dimensioni dell'immagine riempiendo i pixel in posizione $(2x, 2y)$ con lo stesso colore di quelli in posizione (x, y) nell'immagine originale. Ciò genera un'immagine due volte più grande, ma piena di «buchi» e pertanto molto sgranata. (Nessuno dei pixel con almeno una coordinata dispari ha un colore.) Per eliminare questo effetto si potrebbero colorare i pixel rimanenti (quelli con almeno una coordinata dispari) prendendo la media dei valori di colore per tutti i pixel adiacenti che hanno entrambe le coordinate pari. ‘

Questo semplice metodo di riempimento dei buchi funzionerebbe bene per regioni abbastanza omogenee dell'immagine, dove i cambiamenti da un pixel a quello successivo sono piccoli, ma in corrispondenza di un contorno o di un improvviso cambiamento di colore sarebbe disastroso, portando nella migliore delle ipotesi a contorni sfocati e, nella peggiore, a una significativa distorsione (pixelizzazione) dell'immagine. Quando c'è un bordo, ad esempio, ciò che si dovrebbe fare in realtà è

compiere la procedura di calcolo della media lungo il contorno (per preservarne la geometria) e poi fare la media dei colori separatamente nelle regioni ai due lati. In un'immagine con soltanto pochi contorni ben definiti ed essenzialmente dritti, questo lavoro può essere svolto manualmente, ma in un'immagine più tipica si sente l'esigenza di un'individuazione automatica dei bordi. Ciò richiede che il software di elaborazione delle immagini sia in grado di riconoscere i contorni. In pratica, il computer deve essere programmato con la capacità di «comprendere» alcune caratteristiche dell'immagine. Questo si può fare, ma non è facile e richiede alcuni sofisticati strumenti matematici.

La tecnica fondamentale è chiamata segmentazione e consiste nel suddividere l'immagine in regioni distinte che corrispondono a oggetti o a parti di oggetti differenti nella scena originale. (Un caso particolare di segmentazione è la separazione degli oggetti dallo sfondo.) Una volta che l'immagine è stata segmentata, le informazioni mancanti in ogni dato segmento possono essere reintrodotti mediante una tecnica appropriata di calcolo dei valori medi di colore. Esistono svariati metodi per segmentare un'immagine, tutti molto tecnici, ma possiamo comunque descrivere l'idea generale. Dato che le immagini digitali sono visualizzate come matrici rettangolari di pixel, ognuno con una coppia unica di coordinate x,y , qualunque contorno o tratto liscio dell'immagine può essere visto come una curva, definita da una formula algebrica nel senso classico della geometria. Ad esempio, per una linea dritta, i pixel soddisferebbero un'equazione nella forma:

$$y = mx + c$$

Pertanto, un modo per identificare qualunque bordo dritto in un'immagine sarebbe di andare a cercare gli insiemi di pixel dello stesso colore che soddisfano un'equazione di questo tipo e che hanno lo stesso colore dei pixel posti su uno dei due lati della linea, mentre sono di colore diverso rispetto a quelli situati sull'altro lato. Allo stesso modo, i bordi curvilinei potrebbero essere descritti da equazioni matematiche più complesse come le equazioni polinomiali. Naturalmente, in un'immagine digitalizzata, come in una scena reale, le linee non soddisfano mai esattamente un'equazione matematica, e occorre pertanto concedere un ragionevole grado di approssimazione. Ammesso questo, però, ci si può valere del fatto che da un punto di vista matematico qualunque bordo liscio (vale a dire non interrotto da angoli acuti) può essere approssimato, con qualsiasi grado di accuratezza si desideri, da un insieme di (differenti) equazioni polinomiali, ove un'equazione approssima una parte del contorno, un'altra la parte successiva e così via. Questo processo sarà anche in grado di gestire contorni con angoli acuti; in corrispondenza di un angolo, un'equazione polinomiale subentra a quella precedente.

Questa semplice idea mostra come il problema di verificare che un dato contorno è *effettivamente un contorno* possa essere ridotto alla questione di trovare equazioni appropriate. Purtroppo, il fatto di essere in grado di trovare un'equazione la cui curva approssima un segmento di un *dato* contorno non è sufficiente per identificare quel contorno. Per gli esseri umani, riconoscere un contorno non è generalmente un problema. Noi (come altri esseri viventi) possediamo sofisticate abilità cognitive per riconoscere schemi visivi.

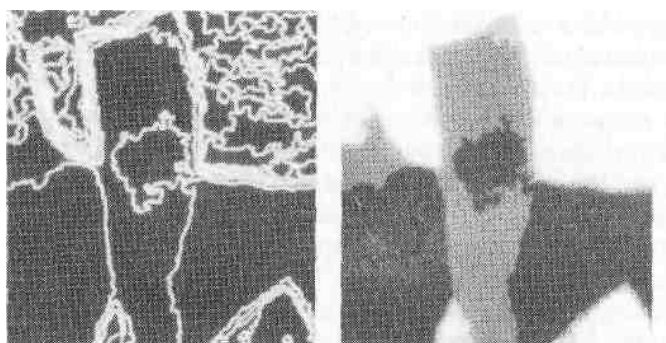


Figura 6. Il risultato dell'algoritmo di segmentazione utilizzato per la fotografia del braccio sinistro dell'aggressore di Reginald Denny: l'immagine elaborata mostra un segno che corrisponde in maniera del tutto verosimile alla rosa tatuata sul braccio sinistro di Williams.

Ma i computer sono privi di tali capacità. Quello in cui eccellono è la manipolazione di numeri e di equazioni. Pertanto, il metodo più promettente per individuare i contorni sembrerebbe essere quello di manipolare le equazioni in qualche modo sistematico finché non se ne trovi una che approssimi il segmento di contorno dato, vale a dire tale per cui le coordinate dei punti sul segmento di contorno soddisfino approssimativamente l'equazione. La figura 6 mostra il risultato dell'algoritmo di segmentazione che la Cognitech applicò alla porzione cruciale della fotografia aerea scattata nel caso del pestaggio di Reginald Denny.

Questo è, in sostanza, il modo in cui funziona la procedura di segmentazione, ma per la sua effettiva messa in opera occorrono mezzi matematici che vanno ben oltre lo scopo di questo libro. Per i lettori che hanno qualche familiarità con la matematica a livello universitario, la sezione che segue offre una breve spiegazione del metodo; i lettori che non hanno questo tipo di preparazione possono tranquillamente passare al paragrafo successivo.

Ottimizzazione di immagini: uno sguardo più ravvicinato

Il processo di ottimizzazione è più facile con le immagini in bianco e nero (più precisamente, in scala di grigio) che non con quelle a colori e quindi ci concentreremo solo su questo caso speciale. Fatta questa restrizione, un'immagine digitale è semplicemente una funzione F da un dato spazio rettangolare (diciamo, una griglia 1000×650) all'intervallo reale unitario $[0,1]$ (vale a dire, i numeri reali tra 0 e 1, 0 e 1 compresi). Se $F(x,y) = 0$, allora il pixel (x,y) è di colore bianco, se $F(x,y) = 1$, il pixel è di colore nero e in tutti gli altri casi $F(x,y)$ denota una sfumatura di grigio tra il bianco e il nero; più grande è il valore di $F(x,y)$, più il pixel (x,y) si avvicina al nero. Praticamente, un'immagine digitale assegna valori della scala di grigio soltanto a un numero finito di pixel; l'immagine consiste in una griglia di pixel. Per applicare la matematica, tuttavia, assumiamo che la funzione $F(x,y)$ sia definita sull'intero rettangolo, ovvero che $F(x,y)$ dia un valore per ogni numero reale x,y all'interno del rettangolo stabilito. Questo ci consente di utilizzare il vasto e potente macchinario del calcolo bidimensionale (ovvero il calcolo di funzioni a valori reali di due variabili

reali).

Il metodo impiegato dalla squadra della Cognitech era basato su un'idea che Rudin concepì durante il suo internato presso i laboratori Bell all'inizio degli anni '80 e che poi sviluppò nella sua tesi di dottorato discussa al California Institute of Technology nel 1987. Ponendosi alcune domande fondamentali sulla percezione visiva - «perché vediamo un unico punto su un foglio di carta?», «come vediamo i contorni?» o «perché abbiamo difficoltà a distinguere le immagini sfocate?» - e collegando queste domande alla funzione matematica corrispondente $F(x,y)$, egli colse l'importanza di quelle che vengono chiamate le singolarità della funzione. Si tratta dei punti in cui la derivata (nel senso del calcolo) diviene infinita. Ciò lo portò a concentrare la sua attenzione su un modo particolare di misurare quanto una determinata funzione sia vicina a una data immagine: la cosiddetta regola della variazione totale. I dettagli sono molto tecnici e non occorre specificarli in questa sede. Il risultato fu che, assieme ai suoi colleghi della Cognitech, Rudin mise a punto tecniche computazionali per restaurare le immagini utilizzando quello che oggi viene chiamato metodo della variazione totale.¹⁰

La matematica in tribunale

Oltre ai loro ovvi usi nei servizi segreti militari, i metodi messi a punto dalla Cognitech trovarono presto applicazioni nell'ottimizzazione delle immagini satellitari per scopi non militari, come l'individuazione di fuoriuscite di petrolio, e nell'elaborazione delle immagini ottenute mediante gli esami di risonanza magnetica per identificare anomalie nei tessuti quali tumori o arterie ostruite. Al tempo del processo contro Damian Williams, la compagnia si era già guadagnata una buona reputazione ed era nella posizione ideale per offrire il suo rivoluzionario contributo.

Oltre che per ricostruire l'immagine cruciale che consentì di identificare Damian Williams come l'uomo che aveva lanciato una lastra di calcestruzzo contro la testa di Denny, Rudin e i suoi colleghi utilizzarono le loro tecniche matematiche anche per ricavare altre immagini fisse di qualità fotografica dal filmato degli eventi, le quali permisero di identificare Williams come il responsabile di aggressioni contro molte altre vittime nei diversi luoghi in cui si era recato quel giorno.

Chiunque abbia osservato un fermo immagine di una videoregistrazione su un videoregistratore, avrà notato che la qualità dell'immagine è estremamente bassa. I sistemi video pensati per usi amatoriali o anche per i reportage giornalistici sfruttano il modo in cui funziona il sistema visivo umano, al fine di ridurre i requisiti di memoria della videocamera. In parole povere, ciascun fotogramma registra solo la metà delle informazioni catturate dall'obiettivo, e il fotogramma successivo registra la (versione aggiornata della) metà mancante. Il nostro sistema visivo fonde automaticamente le due immagini successive per creare un'immagine dall'aspetto realistico in quanto percepisce l'intera sequenza di immagini fisse come se rappresentasse un movimento continuo. Registrare solo metà di ogni immagine

¹⁰ Per chi conosce il lessico matematico, l'idea centrale era di minimizzare il funzionale variazionale totale risolvendo l'equazione di Eulero-Lagrange, una tecnica di calcolo ideata molto prima che entrassero in scena i computer.

funziona bene quando la videoregistrazione risultante viene riprodotta nel suo insieme, ma ciascun singolo fotogramma è di solito estremamente sfocato. L'immagine potrebbe essere migliorata fondendo tra loro due fotogrammi successivi, ma siccome un video registra a una risoluzione molto più bassa (che significa meno pixel) rispetto a una tipica fotografia fissa, il risultato sarebbe ancora di bassa qualità. Per ottenere immagini di qualità fotografica ammissibili in tribunale come prove, Rudin e la sua squadra della Cognitech utilizzarono tecniche matematiche per fondere non due ma molteplici fotogrammi. Tali tecniche erano necessarie perché i vari fotogrammi catturavano l'azione in tempi diversi; se si fossero limitati ad «aggiungerli tutti tra loro», Rudin e i suoi colleghi avrebbero ottenuto un'immagine ancor più sfocata di ogni singolo fotogramma.

La sequenza di immagini fisse fuse prodotta a partire dalle videoregistrazioni sembrava mostrare Williams nell'atto di commettere diverse azioni violente, ma l'identificazione non era sempre decisiva e, come fece notare la difesa, le immagini ricostruite sollevavano apparentemente qualche problema. Ad esempio, alcune immagini mostravano l'impronta di una mano sulla maglietta bianca del criminale che non era visibile nelle immagini precedenti. Il dilemma fu risolto quando un esame attento della videoregistrazione indicò il momento esatto in cui l'impronta della mano era stata prodotta. Fatto ancor più problematico, alcune immagini mostravano una macchia sulla maglietta dell'aggressore che non si vedeva più nelle immagini successive. In quel caso, l'ingrandimento e l'ottimizzazione delle immagini interessate mostrò che nelle inquadrature successive il criminale indossava due magliette bianche, una sopra l'altra, in modo che quella esterna nascondeva la macchia su quella interna. (L'immagine ottimizzata rivelò il lembo della maglietta interna che spuntava sotto il bordo di quella esterna.)

La tecnologia di elaborazione delle immagini video ideata dalla Cognitech svolse un ruolo anche in alcuni altri casi giudiziari che seguirono alle sommosse. In uno di essi, l'imputato, Gary Williams, si dichiarò colpevole di tutti i capi d'accusa dopo la presentazione in tribunale di una videoregistrazione ottimizzata di novanta secondi che lo mostrava mentre rovistava nelle tasche di Denny e mentre compiva altre azioni illegali. Sebbene inizialmente le sue intenzioni fossero di dichiararsi non colpevole e di sottoporsi al giudizio della giuria in un processo, quando lui e il suo avvocato videro il video ottenuto con le tecniche di ottimizzazione convennero che era sufficientemente chiaro da poter essere accolto dalla giuria come prova e optarono per un patteggiamento della pena, che si concluse con una condanna a tre anni di reclusione.

L'avventura continua...

Poche settimane dopo che i casi collegati alle rivolte di Los Angeles stabilirono l'ammissibilità legale delle immagini ottimizzate, la Cognitech fu di nuovo chiamata a offrire i suoi servizi. In quell'occasione, la compagnia fu coinvolta dalla difesa in un caso di rapina a mano armata con sparatoria in una gioielleria. La rapina era stata registrata da una videocamera di sorveglianza. Tuttavia, non solo la risoluzione era

bassa (come accade spesso), ma la videocamera aveva anche registrato alla bassa frequenza di un fotogramma al secondo, molto al di sotto della soglia richiesta per una vera videoregistrazione (più o meno ventiquattro fotogrammi al secondo). Rudin e i suoi colleghi riuscirono a costruire alcune immagini che contraddicevano certe testimonianze presentate al processo. In particolare, le immagini ottenute mostravano che una delle principali testimoni si trovava in una stanza da cui non poteva aver visto quello che sosteneva di aver visto.

Da quel momento in poi, la Cognitech ha continuato a sviluppare i suoi sistemi, e il suo software matematico avanzato Video-Investigator and Video-Active Forensic Imaging è usato oggi da migliaia di esperti nell'ambito dei servizi di polizia e di sicurezza e nei laboratori legali di tutto il mondo, compresi l'FBI, la DEA, l'UK Home Office e Scotland Yard, l'Interpol e molti altri.

In un caso degno di nota, nell'Illinois, un giovane afroamericano era stato dichiarato colpevole (in parte sulla base delle sue stesse parole e in parte sulla base di videoregistrazioni accolte come prove) del brutale assassinio del commesso di un negozio e rischiava la pena di morte. L'accusato e i suoi famigliari erano troppo poveri per potersi permettere costosi servizi di esperti, ma per un caso fortunato il suo pubblico difensore contestò l'identificazione compiuta dai periti statali e federali sulla base delle videoregistrazioni. Il difensore contattò la Cognitech, la quale eseguì un accurato restauro delle immagini e le sottopose poi a una procedura di fotogrammetria tridimensionale (una tecnica che consiste nell'eseguire accurate misurazioni a partire da fotografie, utilizzando le regole matematiche della prospettiva tridimensionale). Ciò rivelò un'indiscutibile discrepanza con le misure fisiche dell'accusato. Conseguentemente, il caso fu chiuso e il giovane innocente rilasciato. Qualche tempo dopo, un'indagine dell'FBI portò alla cattura e alla condanna del vero assassino.

Lavorando con Discovery Channel a uno speciale su alcuni avvistamenti UFO in Arizona (*Lights over Phoenix*), la Cognitech elaborò ed esaminò i videofilmati dimostrando che le «luci» avvistate nel cielo notturno avevano le stesse caratteristiche di quelle emesse dai razzi di segnalazione usati dall'Air Force americana quella notte. Inoltre, lo studio della Cognitech dimostrò che la fonte delle luci si trovava in realtà dietro le montagne, e non sopra Phoenix come avevano pensato inizialmente gli avvistatori.

Più recentemente, lavorando a un altro speciale di Discovery Channel (*Magic Bullet*) sull'assassinio di John Fitzgerald Kennedy, Rudin e la sua squadra utilizzarono le loro tecniche per risolvere il famoso mistero del «secondo tiratore» sul colle erboso. Elaborando la storica fotografia di Mary Moorman con le tecniche più avanzate di restauro delle immagini oggi disponibili, riuscirono a dimostrare che il fantomatico «secondo tiratore» era un artefatto della fotografia, e non una caratteristica stabile dell'immagine. Impiegando tecniche avanzate di fotogrammetria tridimensionale, essi misurarono il misterioso «secondo tiratore» e scoprirono che era alto meno di un metro.

In un'epoca in cui chiunque abbia un'abilità sufficiente è in grado di «rimaneggiare» una fotografia (un processo che dipende anche da sofisticati mezzi matematici), il vecchio detto «le fotografie non mentono» non vale più. Ma grazie

allo sviluppo delle tecniche di ricostruzione delle immagini, vale un nuovo detto: le fotografie (e le videoregistrazioni) generalmente possono dire molto più di quanto si pensi.

PREVEDERE IL FUTURO

L'inferenza bayesiana

Caccia all'uomo

Quando un pullman che trasporta alcuni detenuti resta coinvolto in un incidente stradale, due dei prigionieri scappano, uccidendo la guardia durante la fuga. Charlie contribuisce in qualche modo a sbrogliare la matassa compiendo un'analisi dettagliata della scena dell'incidente, che gli consente di ricostruire che cosa deve essere accaduto. La sua conclusione è che lo scontro non è stato un incidente, ma è stato intenzionalmente organizzato. La fuga era premeditata.

Questa è la storia che gli spettatori di *NUMB3RS* hanno visto nell'episodio della prima serie intitolato *Caccia all'uomo*, mandato in onda in Italia il 1° luglio 2007.

La ricostruzione matematica dell'incidente inscenata da Charlie si basa sul modo in cui operano nella vita reale quelli che indagano sugli incidenti stradali. Ma il coinvolgimento di Charlie in questo caso particolare non si limita a cercare di capire come sia avvenuto l'incidente. Dopo che uno dei fuggitivi viene catturato, l'attenzione si concentra sul trovare l'altro, l'uomo che ha pianificato la fuga. Si scopre che il prigioniero catturato, un prigioniero modello che aveva quasi finito di scontare la sua pena, non era a conoscenza del piano di fuga. Ma egli è in grado di parlare a Don del suo compagno, un assassino condannato all'ergastolo senza condizionale, e pertanto un soggetto altamente pericoloso che aveva poco da perdere nel compiere un altro omicidio. La cosa più agghiacciante che il prigioniero dice a Don è che l'assassino intende uccidere il principale testimone al suo processo, una donna la cui testimonianza aveva contribuito a condannarlo.

Don cerca di persuadere la testimone a lasciare la città e a nascondersi finché l'assassino è in circolazione, ma lei rifiuta. E un medico ospedaliero con pazienti da cui sente di non potersi allontanare. Ciò costringe Don a una corsa contro il tempo per ritrovare il fuggitivo prima che possa portare a compimento il suo disegno di morte.

Le notizie della fuga divulgate dai mass media, che comprendevano fotografie dell'assassino evaso, portano presto a diverse segnalazioni di avvistamenti da parte della popolazione. Purtroppo le segnalazioni arrivano in massa, diverse centinaia in totale, e sono sparse per tutta Los Angeles, spesso riportando avvistamenti simultanei in luoghi situati a diversi chilometri di distanza. Per quanto alcune possano essere degli scherzi, la maggior parte proviene probabilmente da cittadini benintenzionati che davvero credono di aver individuato l'uomo che hanno visto sui giornali o in televisione. Ma come può Don decidere quali avvistamenti sono attendibili, o per lo meno quali hanno più probabilità di esserlo?

E qui che Charlie offre il suo secondo contributo. Egli afferma di aver condotto

un'«analisi statistica bayesiana» degli avvistamenti, che gli dice quali sono più probabilmente attendibili. Utilizzando i risultati di Charlie, Don è in grado di determinare dove si trova probabilmente l'assassino, e riesce a raggiungerlo appena in tempo per evitare che uccida la testimone.

Come accade spesso nelle rappresentazioni della matematica o della scienza in azione, il tempo che Charlie impiega per produrre la classificazione degli avvistamenti segnalati è notevolmente abbreviato, ma l'idea di utilizzare la tecnica matematica nota come analisi statistica bayesiana è ben fondata. Alla fine di questo capitolo, spiegheremo come è più probabile che Charlie abbia eseguito la sua analisi. (Gli spettatori non vedono compiere questo passaggio, e il copione non offre dettagli.) Prima, però, dobbiamo descrivere in termini più generali le importantissime tecniche della statistica bayesiana.

Prevedere il futuro

Il lavoro delle forze di polizia sarebbe molto più semplice se potessimo guardare nel futuro ed essere a conoscenza dei crimini prima che avvengano realmente.¹¹ Ma anche con l'aiuto della matematica ciò non è possibile. La matematica può prevedere, con il grado di accuratezza desiderato, che posizione avrà un veicolo spaziale che viaggia a migliaia di chilometri l'ora tra sei mesi a mezzogiorno, ora media di Greenwich, ma la maggior parte di noi trova difficile prevedere con precisione dove si troverà anche solo tra una settimana a mezzogiorno. Il comportamento umano, semplicemente, non è suscettibile di previsione matematica. Per lo meno, non se si vuole che la matematica dia una risposta esatta. Se, però, ci vogliamo accontentare di stime numeriche su cosa *probabilmente* accadrà, allora la matematica può essere molto utile.

Ad esempio, nessuno, a parte il manipolo di militanti di al-Qaeda che compì gli attacchi dell'11 settembre 2001, sapeva in anticipo che cosa sarebbe successo. Ma le cose avrebbero potuto andare in maniera molto diversa se le autorità statunitensi avessero saputo che tale attacco era probabile, quali erano i bersagli più probabili, e quali azioni intraprendere per impedire ai terroristi di realizzare il loro piano. Può la matematica aiutare a fornire un simile avvertimento anticipato sulle cose che potrebbero succedere, magari con una qualche misura numerica della loro probabilità?

La risposta è che non solo essa può farlo, ma che in quell'occasione lo fece davvero. Un anno prima dell'attacco, alcuni matematici avevano predetto che il Pentagono costituiva un probabile bersaglio dei terroristi. In quell'occasione, nessuno prese la previsione matematica abbastanza sul serio da fare qualcosa a riguardo. Ovviamente, è sempre più facile essere furbi dopo che un evento è accaduto. Quello che la matematica può fare - e fece - è produrre un elenco di bersagli probabili, unitamente alle stime delle probabilità che un attacco abbia luogo. Agli strateghi

¹¹ Questa era l'idea principale dietro la trama del popolare film del 2002 *Minority Report*, con Tom Cruise. Ma, naturalmente, è solo finzione.

politici resta da decidere su quali delle molte minacce identificate si dovrebbero investire le limitate risorse disponibili. Ma, considerato il modo in cui si svolsero gli eventi in quel fatidico giorno del 2001, forse la prossima volta le cose andranno diversamente.

Come la matematica predisse l'attacco al Pentagono dell'11 settembre

Nel maggio del 2001, un sistema software chiamato Site Profiler fu fornito a tutte le installazioni militari statunitensi in giro per il mondo. Il software dotava i comandanti delle varie postazioni di strumenti che aiutavano a valutare i rischi di attacchi terroristici, a gestire tali rischi e a mettere a punto piani antiterrorismo standardizzati. Il sistema lavorava combinando diverse fonti di dati per trarre inferenze circa i rischi di attacchi terroristici, utilizzando una tecnica matematica chiamata inferenza bayesiana.

Prima di diffondere il sistema, i suoi ideatori eseguirono un gran numero di test di simulazione, cui fecero riferimento in un articolo che scrissero l'anno precedente.¹² Riassumendo i risultati dei test, fecero notare che «sebbene questi scenari mostrassero che il RIN (*Risk Influence Network*) 'funzionava', tendevano a essere eccezionali (ad esempio, attacchi contro il Pentagono)».

Come oggi tutti sappiamo, il Pentagono fu sede di un attacco. Purtroppo, né il comando militare né il governo degli Stati Uniti avevano preso sul serio la previsione di Site Profiler che il Pentagono era in pericolo, e nemmeno lo avevano fatto gli stessi ideatori del sistema che avevano considerato la previsione «eccezionale».

Come l'esperienza ci ha insegnato più e più volte, gli esseri umani sono bravi a valutare certi tipi di rischi - in genere, i rischi personali associati a situazioni familiari - ma sono notoriamente molto meno bravi a valutarne altri, in particolare quelli di nuovi tipi di eventi. La matematica non ha un simile punto debole. Le regole matematiche che gli ideatori di Site Profiler costruirono nel sistema non avevano un innato «fattore di incredulità». Il sistema semplicemente macinava numeri, assegnando rischi numerici a vari eventi, e riportava quelli che in base ai calcoli risultavano più probabili. Quando i numeri dissero che il Pentagono era a rischio, questo è ciò che il programma riferì. Furono gli esseri umani a liquidare la previsione come troppo inverosimile.

Questa storia ci insegna due cose. La prima è che la matematica fornisce un potente strumento per valutare i rischi di attacco terroristico. La seconda è che gli esseri umani dovrebbero pensare molto attentamente prima di accantonare i risultati prodotti dai calcoli matematici, indipendentemente da quanto folli possano sembrare.

Questa è la storia che sta dietro a quel tipo di matematica.

¹² *An Application of Bayesian Networks to Antiterrorism Risk Management for Military Planners*, di Linwood D. Hudson, Bryan S. Ware, Suzanne M. Mahoney e Kathryn Blackmond Laskey.

Site Profiler

Site Profiler fu autorizzato dal dipartimento della Difesa statunitense nel 1999 per sviluppare un sistema integrato di gestione del rischio terroristico chiamato Joint Vulnerability Assessment Tool (JVAT).

Il programma JVAT fu avviato in risposta all'attentato contro i membri dell'Air Force americana alle Khobar Towers, in Arabia Saudita, nel giugno del 1996, nel corso del quale furono uccisi 19 militari americani e uno saudita e 372 uomini di diverse nazionalità rimasero feriti, e a quelli dell'agosto 1998 alle ambasciate statunitensi in due capitali dell'Africa orientale, Dar es Salaam in Tanzania e Nairobi in Kenya, in cui persero la vita 257 persone e 4000 rimasero ferite.

Le indagini su questi eventi rivelarono che gli Stati Uniti avevano metodi inadeguati per valutare i rischi di attacco terroristico e anticipare futuri episodi terroristici. Affrontare quel bisogno costituiva una grossa sfida. Dal momento che le intenzioni, i metodi e le risorse di potenziali terroristi, e spesso persino la loro identità, non possono quasi mai essere previsti con certezza a partire dalle informazioni disponibili, gran parte dello sforzo di contrastare la minaccia deve concentrarsi sull'identificazione dei probabili bersagli. Conoscere i punti deboli di un potenziale bersaglio e sapere come difendersi dagli attacchi richiede propriamente il contributo di vari esperti: esperti della sicurezza fisica, ingegneri, scienziati e strateghi militari. Per quanto un numero ristretto di esperti possa essere in grado di comprendere e gestire uno o due rischi particolari, nessun essere umano può controllare tutte le componenti di centinaia di rischi simultaneamente. La soluzione consiste nell'utilizzare metodi matematici implementati su computer.

Site Profiler è soltanto uno dei molti sistemi che consentono agli utenti di stimare con un certo grado di precisione e gestire un grande «portafoglio rischi» usando l'inferenza bayesiana (implementata nella forma di una rete bayesiana, che descriveremo più avanti) per combinare prove che arrivano da diverse fonti di dati: modelli analitici, simulazioni, dati storici e giudizi dell'utente.

Normalmente, chi fa uso di un simile sistema (spesso un'esperta squadra di valutazione) introduce informazioni, poniamo, sui punti di forza di un'installazione militare attraverso un'interfaccia domanda-risposta che ricorda quella di un pacchetto software per la dichiarazione dei redditi. (L'interfaccia di Site Profiler è infatti modellata su quella di Turbo Tax.) Con le informazioni che ha raccolto, il software costruisce oggetti matematici per rappresentare i vari punti forti e deboli dell'installazione, per descrivere l'intera situazione nella forma di una rete bayesiana, per usare la rete in modo da valutare i vari rischi, e infine per produrre una lista di minacce, ognuna associata a un punteggio numerico sulla base della sua probabilità, della gravità delle sue conseguenze e così via. Ciò che ci interessa qui è la matematica che si cela «sotto il velo» di tale sistema. L'idea centrale risale a un pastore presbiteriano inglese del XVIII secolo, Thomas Bayes.

Thomas Bayes e le probabilità di ciò che sappiamo

Oltre a essere un ministro presbiteriano, Thomas Bayes (1702-1761) era un appassionato di matematica. Era affascinato dal modo in cui veniamo a sapere le cose che sappiamo, nello specifico da come giudichiamo l'attendibilità delle informazioni acquisite, e si chiedeva se la matematica potesse essere usata per rendere tali giudizi più precisi e accurati. Il suo metodo per calcolare come le nostre credenze circa le probabilità dovrebbero essere modificate ogni volta che otteniamo nuove informazioni - nuovi *dati* - portò allo sviluppo della statistica bayesiana, un approccio alla teoria e alla pratica dell'analisi statistica che ha attratto per molto tempo ferventi seguaci, così come strenui oppositori. Oggi, dopo l'avvento nel tardo XX secolo di computer immensamente potenti in grado di masticare milioni di dati al secondo, sia gli statistici bayesiani (che utilizzano *sempre* la sua idea fondamentale), sia quelli non bayesiani (che la usano *qualche volta*) pagano nei suoi confronti un grosso debito.

Il metodo di Bayes

L'idea di Bayes riguarda le probabilità di cose che potrebbero essere vere oppure no, come il fatto che la probabilità che esca testa se si lancia una moneta sia compresa tra 0,49 e 0,51, che il farmaco Y faccia passare il mal di testa più frequentemente del farmaco X, che un terrorista o un criminale attaccherà il bersaglio J, K o L. Se vogliamo confrontare due possibilità, A e B, Bayes offre la seguente ricetta:

1. Stimare le loro probabilità relative $P(A)/P(B)$, cioè la probabilità di A rispetto a B.
2. Per ogni nuova osservazione, X, calcolare la probabilità di quell'osservazione se A è vero e se B è vero.
3. Stimare nuovamente le probabilità relative di A e B come segue:
 $P(A \text{ dato } X)/P(B \text{ dato } X) = P(A)/P(B) \times \text{rapporto di verosimiglianza}$, ove il rapporto di verosimiglianza è la probabilità di osservare X se A è vero diviso per la probabilità di osservare X se B è vero.
4. Ripetere il processo ogni volta che si presenta una nuova osservazione.

Le probabilità relative di A e B nel primo passaggio sono chiamate «probabilità a priori», a significare che rappresentano il nostro stato di conoscenza prima di osservare i dati X. Spesso questa conoscenza si basa su giudizi soggettivi: ad esempio, qual è la probabilità che un nuovo farmaco sia migliore di quello normalmente usato per una data malattia? Oppure, qual è la probabilità che i terroristi attacchino un bersaglio piuttosto che un altro? O magari, anche, qual è la probabilità che un imputato sia colpevole, prima che sia presentata qualunque prova? (L'arbitrarietà che sarebbe implicata nel fatto di attribuire un numero nell'ultimo esempio è la ragione per cui l'uso della statistica bayesiana nei processi penali è

praticamente pari a zero!)

Per comprendere la ricetta di Bayes, è utile considerare un esempio in cui queste «probabilità a priori» sono effettivamente note. In una situazione del genere, l'uso dei metodi bayesiani non presenta problemi.

Il caso (fittizio) dell'incidente con omissione di soccorso

Una città ha due compagnie di taxi, i Taxi Blu e i Taxi Neri, la prima con quindici taxi e la seconda con settantacinque. Una notte, un taxi rimane coinvolto in un incidente e fugge senza soccorrere le vittime. I novanta taxi della città erano tutti in circolazione all'ora dell'incidente. Un testimone che ha assistito alla scena afferma che il taxi coinvolto era blu. Su richiesta della polizia, il testimone si sottopone a un esame della vista in condizioni simili a quelle della notte in questione. Posto ripetutamente di fronte a taxi blu e neri, in ordine casuale, egli dimostra di essere in grado di identificare correttamente il colore del taxi quattro volte su cinque (nel restante 20 per cento delle volte, confonde un taxi blu con uno nero e viceversa). Se foste voi a compiere le indagini sul caso, quale compagnia pensereste sia stata più probabilmente coinvolta nell'incidente?

Dinanzi alla dichiarazione di un testimone oculare che ha dimostrato di essere in grado di identificare correttamente il colore dei taxi quattro volte su cinque, potreste essere portati a credere che effettivamente ciò che egli ha visto era un taxi blu. Potreste persino pensare che la probabilità che il taxi fosse blu sia $4/5$ (vale a dire, 0,8), essendo questa la probabilità che il testimone identifichi il colore correttamente in ogni prova.

Il metodo di Bayes dimostra che le cose stanno un po' diversamente. In base ai dati forniti, la probabilità che l'incidente sia stato causato da un taxi blu è solo $4/9$, vale a dire il 44 per cento. Proprio così, la probabilità è inferiore al 50 per cento. E più probabile che il taxi coinvolto fosse nero. Dio aiuti il padrone della compagnia dei taxi blu se i giurati non riescono a seguire il ragionamento bayesiano!

Ciò che l'intuito umano spesso ignora, ma che la regola di Bayes tiene adeguatamente in considerazione, è la probabilità di cinque a uno che qualunque taxi particolare nella città sia nero. Il calcolo bayesiano procede come segue:

1. La «probabilità a priori» che un taxi sia nero è cinque a uno (75 taxi neri contro 15 blu).

La probabilità di $X = \text{«il testimone identifica il taxi come blu»}$ è: 1 su 5 (20%) se è nero 4 su 5 (80%) se è blu.

2. Il nuovo calcolo della probabilità che il taxi fosse nero anziché blu è il seguente:

$P(\text{il taxi era nero data l'identificazione del testimone})/P(\text{il taxi era blu data l'identificazione del testimone}) =$

$$(5/1) \times (20\% / 80\%) = (5 \times 20\%) / (1 \times 80\%) = 1/0,8 = 5/4.$$

Pertanto, il calcolo bayesiano indica che la probabilità che il taxi fosse nero, data la

dichiarazione del testimone, è di cinque a quattro.

Se questo vi sembra controintuitivo (come accade all'inizio ad alcune persone) provate a effettuare il seguente «esperimento mentale». Fate uscire ognuno dei 90 taxi in notti successive e chiedete al testimone di identificare il colore di ciascuno nelle stesse condizioni di prima. Quando appaiono i 15 taxi blu, l'80 per cento delle volte essi vengono descritti come blu, e ci possiamo quindi aspettare 12 «avvistamenti blu» e 3 «avvistamenti neri». Quando escono i 75 taxi neri, il 20 per cento delle volte essi sono descritti come blu, e ci possiamo quindi aspettare 15 «avvistamenti blu» e 60 «avvistamenti neri». Complessivamente, possiamo aspettarci che 27 taxi siano identificati dal testimone come «blu», anche se solo 12 di essi erano effettivamente blu e gli altri 15 erano neri. Il rapporto 12 contro 15 equivale a 4 contro 5: in altre parole, solo 4 volte su 9 (il 44 per cento delle volte) quando il testimone dice di aver visto un taxi blu esso era effettivamente blu.

In uno scenario artificiale in cui le stime iniziali sono totalmente accurate, una rete bayesiana ci fornirà una risposta accurata. In una situazione reale più tipica non disponiamo di cifre esatte per le probabilità a priori, ma se le nostre stime iniziali sono ragionevolmente buone, il metodo terrà conto delle prove disponibili per offrirci una stima *migliore* della probabilità che l'evento in questione si verifichi. Pertanto, nelle mani di un esperto che sia in grado di valutare l'attendibilità di tutte le prove disponibili, le reti bayesiane possono costituire uno strumento efficace.

A caccia dell'assassino evaso

Come abbiamo accennato all'inizio del capitolo, nulla nell'episodio di *NUMB3RS Caccia all'uomo* spiega come Charlie abbia analizzato i vari avvistamenti del prigioniero evaso che erano stati segnalati. A parte dichiarare di aver usato un'«analisi statistica bayesiana», Charlie non dice nulla riguardo al suo metodo. Ma, quasi sicuramente, questo è ciò che deve aver fatto.

Il problema, ricordiamo, è che ci sono tantissime segnalazioni di avvistamenti, molte delle quali contraddittorie. La maggior parte sarà il risultato di persone che hanno visto qualcuno che credono assomigli all'uomo mostrato sui giornali o in televisione. Non è che gli informatori manchino di credibilità; semplicemente si stanno sbagliando. Pertanto la sfida è come fare a distinguere gli avvistamenti corretti dai falsi allarmi, specialmente se si considera che quasi sicuramente i secondi sono in numero di gran lunga superiore.

Il fattore chiave di cui Charlie può valersi discende dal fatto che ogni segnalazione è associata a un orario, quello del presunto avvistamento. Le segnalazioni corrette, indicando tutte avvistamenti del vero assassino, faranno riferimento a luoghi della città disposti secondo uno schema geometrico tale da riflettere gli spostamenti di un singolo individuo. D'altro canto, è probabile che le false segnalazioni facciano riferimento a luoghi distribuiti per la città in una maniera piuttosto casuale, inconciliabile con l'ipotesi che derivino dagli spostamenti di un'unica persona. Ma come fare a selezionare gli avvistamenti che corrispondono a quello schema

nascosto?

Questo non può essere fatto in modo preciso. Ma il teorema di Bayes offre un metodo per assegnare una probabilità ai vari avvistamenti di modo che più alta è la probabilità, più è verosimile che quel particolare avvistamento sia corretto. Vediamo ora quello che Charlie deve aver fatto.

Prendiamo una mappa di Los Angeles. Lo scopo è di assegnare a ciascun quadrato della griglia sulla mappa con coordinate i,j , un valore di probabilità $p(i,j,n)$ che valuti la probabilità che l'assassino si trovi nel quadrato (i,j) all'ora n . L'idea è di usare il teorema di Bayes per aggiornare ripetutamente le probabilità $p(i,j,n)$ nel tempo (ovvero, al crescere di n), poniamo a intervalli di cinque minuti.

Per iniziare il processo, Charlie deve assegnare delle probabilità iniziali a priori a ciascun quadrato della griglia. La cosa più verosimile è che determini tali probabilità in base alla testimonianza del prigioniero catturato riguardo a dove e quando i due si sono separati. Senza tale informazione, potrebbe semplicemente assumere che le probabilità dei quadrati della griglia siano tutte uguali.

A ogni intervallo temporale successivo, Charlie calcola la nuova distribuzione delle probabilità a posteriori nel modo seguente. Prende ogni nuova segnalazione - un avvistamento nel quadrato (i,j) all'ora $n+1$ - e sulla sua base aggiorna le probabilità di tutti i quadrati (x,y) , utilizzando la probabilità di quell'avvistamento se l'assassino si fosse trovato nel quadrato (x,y) all'ora n . Chiaramente, per $(x,y) = (i,j)$, Charlie calcola un'alta probabilità per l'avvistamento all'ora $n+1$, in particolare se la segnalazione riferisce che l'assassino stava facendo qualcosa che avrebbe richiesto del tempo, come consumare un pasto o farsi tagliare i capelli.

Anche se (x,y) è vicino a (i,j) , la probabilità calcolata da Charlie che l'assassino si trovi nel quadrato (i,j) all'ora $n+1$ è alta, in particolare se la segnalazione riferisce che l'assassino era a piedi, il che rende improbabile che sia potuto andare lontano in un intervallo temporale di cinque minuti. La probabilità esatta assegnata da Charlie può variare a seconda di ciò che, in base a quanto riferito dalla segnalazione, l'individuo stava facendo. Ad esempio, se viene riferito che l'individuo all'ora n stava «guidando verso nord su Third Street», Charlie attribuisce ai quadrati a nord di Third Street una probabilità più alta di avvistamento all'ora $n+1$ rispetto ai quadrati situati altrove.

Presumibilmente le probabilità assegnate da Charlie tengono anche conto delle stime di veridicità. Ad esempio una segnalazione proveniente dal sorvegliante di una banca, che offre una descrizione piuttosto dettagliata, avrà maggiori probabilità di essere corretta di una che arriva da un ubriaco in un bar, fatto che indurrà Charlie ad assegnare probabilità più alte a quanto viene riferito dal primo testimone. Pertanto, la probabilità che l'assassino si trovi nel quadrato (x,y) all'ora $n+1$ sulla base di una segnalazione attendibile che riferisce che si trovava nel quadrato (i,j) all'ora n è molto più alta se (x,y) è vicino a (i,j) che non nel caso in cui i due quadrati siano più lontani, mentre nel caso di una segnalazione meno attendibile, la probabilità di un avvistamento nel quadrato (i,j) è più «generica» e meno dipendente da (x,y) .

Molto probabilmente Charlie tiene in considerazione anche qualche altro fattore. Ad esempio, un grande centro commerciale la domenica pomeriggio probabilmente darà origine a più false segnalazioni di un'area industriale il martedì sera.

Tale processo, naturalmente, dipende molto dalle valutazioni e dalle stime umane. Da solo, porterebbe difficilmente a qualche conclusione utile. Ma è qui che entra in gioco il potere del metodo bayesiano. Il gran numero di avvistamenti, che a prima vista sembrava un problema, diviene ora un vantaggio significativo. Per quanto la distribuzione delle probabilità che Charlie assegna alla mappa a ogni intervallo temporale sia altamente soggettiva, essa è basata su un fondamento logico *razionale*, e la precisione matematica del teorema di Bayes, quando viene applicato molte volte, alla fine supera la vaghezza intrinseca a ogni stima umana. Di fatto, quello che fa l'applicazione ripetuta del teorema di Bayes è estrapolare lo schema nascosto derivante dal fatto che i veri avvistamenti dell'assassino erano tutti avvistamenti dello stesso individuo man mano che si muoveva per la città.

In altre parole, il paradigma bayesiano fornisce a Charlie un solido mezzo quantitativo per considerare simultaneamente tutti i luoghi possibili a ogni intervallo temporale. Naturalmente, ciò che egli ottiene non è una singola croce sulla mappa, ma una distribuzione di probabilità. Tuttavia, nel corso del processo, potrebbe raggiungere qualche stadio in cui vengono assegnate alte probabilità a due o tre luoghi plausibili sulla base di recenti segnalazioni. Se a quel punto egli ricevesse due o tre segnalazioni attendibili che collimano, la formula di Bayes potrebbe attribuire un'alta probabilità a uno di quei luoghi. Quindi Charlie contatterebbe suo fratello Don e direbbe: «Manda subito lì un agente!»

IL TEST DEL DNA

Di questi tempi si sente spesso parlare del test del DNA, un metodo usato per identificare le persone. Sebbene la tecnica sia spesso descritta in termini di «impronta digitale genetica» non ha nulla a che vedere con le impronte digitali. Piuttosto, il termine popolare rimanda a un mezzo più vecchio, e più affermato, per identificare le persone. Benché entrambi i metodi siano altamente accurati, in ambedue i casi bisogna stare attenti a calcolare la probabilità di una falsa identificazione risultante dal fatto che due individui diversi hanno impronte digitali (di uno o dell'altro tipo) che il test non è in grado di distinguere. E qui che entra in gioco la matematica.

Stati Uniti d'America contro Raymond Jenkins

Il 4 giugno 1999 alcuni poliziotti di Washington trovarono il corpo di un cinquantunenne di nome Dennis Dolinger nella sua casa a Capitol Hill. Era stato pugnalato molte volte - almeno venticinque secondo i verbali - con un cacciavite che gli aveva penetrato il cervello.

Dolinger era stato un analista di gestione presso l'autorità dei trasporti pubblici di Washington e aveva vissuto a Capitol Hill per vent'anni svolgendo un ruolo attivo nella comunità. Aveva un'ampia rete di amici e colleghi in tutta la città. In particolare, si era spesso impegnato politicamente in questioni di interesse locale e aveva preso una ferma posizione contro lo spaccio di droga nella zona.

La polizia trovò una traccia di sangue che portava dal seminterrato dove fu ritrovato Dolinger al primo e al secondo piano della sua casa e al vialetto e al marciapiede di fronte. Abiti insanguinati furono ritrovati nel seminterrato e in una stanza al secondo piano. La polizia pensò che alcune delle macchie di sangue fossero dell'assassino, che si era tagliato durante l'aggressione. Il portafogli di Dolinger, contenente denaro e carte di credito, era stato rubato, e mancavano anche il suo anello di diamanti e la sua catenina d'oro.

La polizia identificò presto diversi sospetti: il precedente fidanzato di Dolinger (Dolinger era dichiaratamente omosessuale), che lo aveva aggredito in passato e che aveva lasciato l'area di Washington, DC, più o meno quando la polizia aveva ritrovato il corpo; un uomo che era stato visto fuggire dalla casa di Dolinger ma che non aveva chiamato la polizia; alcuni spacciatori di droga della zona, tra cui uno contro cui Dolinger aveva testimoniato nel corso di un processo per omicidio; alcuni vicini che avevano commesso atti di violenza contro gli animali domestici di Dolinger; vari senzatetto che facevano frequentemente visita a Dolinger e alcuni omosessuali che Dolinger aveva incontrato in qualche bar o attraverso servizi di appuntamenti in Internet.

La pista più promettente si aprì quando un uomo di nome Stephen Watson utilizzò una delle carte di credito di Dolinger da un parrucchiere e in un grande magazzino ad Alexandria entro quindici ore dalla sua morte. Watson era un tossicodipendente con una lunga fedina penale, che includeva reati inerenti il possesso e lo spaccio di droghe, violazioni di proprietà e aggressioni. La polizia parlò con un testimone che conosceva Watson di persona e che lo aveva visto il giorno dell'omicidio nelle vicinanze della casa di Dolinger «con un aspetto nervoso e agitato», con un «pezzo di stoffa avvolto attorno alla mano» e addosso «una maglietta macchiata di sangue». Anche un altro testimone aveva visto Watson nelle vicinanze della casa di Dolinger il giorno dell'omicidio, notando che aveva con sé diverse carte di credito.

Il 9 giugno, la polizia si recò nella casa di Watson ad Alexandria, in Virginia, con un mandato di perquisizione e trovò alcuni documenti personali appartenenti a Dolinger. Gli agenti notarono anche che Watson, il quale era presente durante la perquisizione, aveva un taglio sul dito «che sembrava essere stato prodotto diversi giorni prima e stava iniziando a guarire». A quel punto, la polizia lo arrestò. Quando fu interrogato alla stazione di polizia, Watson «inizialmente negò di conoscere il defunto e di aver usato la carta di credito», ma poi disse che «aveva trovato un portafogli in uno zaino abbandonato vicino a una scarpata accanto a un'incerata beige e a dei secchi in King Street» ad Alexandria. Sulla base di questi fatti, la polizia accusò Watson di omicidio indiretto.

Questa potrebbe sembrare la fine della storia: un caso inequivocabile, si potrebbe pensare. Ma le cose stavano per diventare assai più complicate. L'FBI aveva estratto e analizzato il DNA di vari campioni di sangue raccolti sulla scena del delitto e nessuno di essi corrispondeva a quello di Watson. Di conseguenza, l'US Attorney's Office lasciò cadere l'accusa contro Watson, il quale fu rilasciato.

A questo punto dobbiamo dare un'occhiata al metodo di identificazione sulla base del DNA, una procedura nota come determinazione del profilo genetico.

Il profilo genetico

La molecola di DNA è composta da due lunghi filamenti, attorcigliati l'uno attorno all'altro nella oggi familiare struttura a doppia elica e uniti assieme alla stregua di una scala di corda mediante blocchi di costruzione chimici chiamati basi (i due filamenti costituiscono le «corde» laterali della «scala», mentre i legami tra le basi formano i «pioli»). Esistono quattro tipi diversi di basi: adenina (A), timina (T), guanina (G) e citosina (C). Il genoma umano consiste di una sequenza di circa tre miliardi di queste coppie di basi. Procedendo lungo la molecola di DNA, la sequenza di lettere denotante l'ordine delle basi (una porzione potrebbe essere ... AATGGGCATTTTGAC...) fornisce una «lettura» del codice genetico dell'individuo (o dell'essere vivente) esaminato. E questa «lettura» a fornire la base per la determinazione del profilo genetico.

Il DNA di ogni persona è unico; se si conoscesse con esattezza l'intera sequenza di tre miliardi di lettere che forma il DNA di un dato individuo si saprebbe chi è quella persona, senza possibilità di errore. Tuttavia, utilizzando le tecniche attuali, e con

tutta probabilità anche quelle future, è assolutamente impossibile effettuare un'identificazione del DNA determinando tutti i tre miliardi di lettere. Ciò che viene fatto, invece, è un esame di una piccolissima manciata di siti di variazione, con l'ausilio della matematica per stabilire l'accuratezza dell'identificazione risultante.

Il DNA è organizzato in grandi corpi strutturali chiamati cromosomi. Gli esseri umani possiedono ventitré coppie di cromosomi che assieme costituiscono il genoma umano. In ogni coppia, un cromosoma è ereditato dalla madre e uno dal padre. Ciò significa che un individuo avrà due assetti completi di materiale genetico. Un «gene» è in realtà una collocazione (locus) su un cromosoma. Alcuni geni possono avere differenti versioni, chiamate «alleli». I due cromosomi di una data coppia hanno gli stessi loci per tutta la loro lunghezza, ma possono avere alleli diversi in corrispondenza di alcuni loci. Gli alleli sono caratterizzati da sequenze di basi leggermente diverse e si distinguono per i loro differenti effetti fenotipici. Alcuni dei geni studiati nei test del DNA in ambito medico-legale hanno ben trentacinque alleli differenti. La maggior parte delle persone possiede loci molto simili, ma alcuni variano da individuo a individuo con un'elevata frequenza. Il confronto delle variazioni in questi loci permette agli scienziati di capire se due differenti campioni di DNA provengano o meno dalla stessa persona. Se i due profili sono uguali in ciascuno dei loci esaminati, si dice che corrispondono. Se differiscono per uno o più loci, i due profili non corrispondono, ed è praticamente certo che i campioni non provengono dalla stessa persona.¹³

Una corrispondenza non implica che due campioni debbano necessariamente provenire dalla stessa fonte; tutto quello che si può dire è che, per quanto il test è stato in grado di determinare, i due profili sono identici, ma è possibile che più di una persona abbia lo stesso profilo in diversi loci. Per ogni locus, la percentuale di persone con tratti di DNA corrispondenti è piccola ma non nulla.

I test del DNA traggono la loro forza dalla presenza simultanea di corrispondenze in ciascuno di numerosi loci, essendo estremamente raro che due campioni presi da individui senza alcun rapporto di parentela mostrino una simile congruenza in un gran numero di loci. E qui che entra in gioco la matematica.

Il sistema CODIS dell'FBI

Nel 1994, riconoscendo l'importanza crescente delle analisi del DNA in ambito medico-legale, il Congresso degli Stati Uniti promulgò il DNA Identification Act, che autorizzava la creazione di una banca dati nazionale di tutti i detenuti americani e istituiva il DNA Advisory Board (DAB) per dare consigli in materia all'FBI.

Il sistema CODIS (*Combined DNA Index System*), l'archivio dei profili genetici dell'FBI, era stato avviato come programma pilota nel 1990. Il sistema combina tecnologie informatiche e genetiche per fornire un potente strumento di lotta contro il crimine. Questa banca dati di DNA comprende quattro categorie di archivi:

¹³ Il confronto non viene effettuato direttamente tra le sequenze dei quattro tipi di basi, ma su conteggi numerici delle basi. Il «profilo genetico» è in realtà una sequenza di questi conteggi. Ma tale distinzione non è importante per i nostri scopi.

- *Detenuti*: archivi di identificazione genetica di persone condannate per crimini.
- *Archivio medico-legale*: analisi di campioni di DNA recuperati dalle scene dei delitti.
- *Resti umani non identificati*: analisi di campioni di DNA raccolti da resti umani non identificati.
- *Parenti di persone scomparse*: analisi di campioni di DNA forniti volontariamente dai parenti di persone scomparse.

La banca dati CODIS dei detenuti contiene attualmente più di tre milioni di dati.

I profili del DNA archiviati nel sistema CODIS si basano su tredici loci specifici, selezionati perché esibiscono una considerevole variazione nell'ambito della popolazione.

Il sistema utilizza un software informatico per compiere ricerche automatiche all'interno di queste banche dati al fine di rintracciare corrispondenze nei profili genetici. Il sistema mantiene anche un file di popolazione: una banca dati di profili genetici anonimi usata per determinare la significatività statistica di una corrispondenza.

CODIS non è una banca dati di criminali completa, ma solo un sistema di indicazioni; esso contiene solo le informazioni necessarie per stabilire delle corrispondenze. I profili archiviati nel sistema CODIS contengono l'identificativo del campione, l'indicazione del laboratorio finanziatore, le iniziali (o il nome) del personale che ha compiuto l'analisi e le effettive caratteristiche del DNA. L'archivio non contiene informazioni sulla fedina penale dell'individuo o sul caso giudiziario in cui è stato coinvolto, né riporta dati personali come numero di previdenza sociale o data di nascita.

Quando due campioni di DNA scelti a caso corrispondono completamente in un gran numero di regioni, come i tredici loci impiegati nel sistema CODIS, la probabilità che essi provengano da due persone senza alcuna parentela è praticamente pari a zero. Questo fatto rende l'identificazione basata sul DNA estremamente affidabile (quando effettuata correttamente). Il grado di affidabilità viene generalmente calcolato utilizzando la teoria della probabilità per determinare quanto sia probabile trovare un particolare profilo in un campione casuale della popolazione.

Torniamo al caso Jenkins

Dopo che il primo sospetto fu scagionato perché il suo profilo genetico non corrispondeva a nessuno dei campioni ritrovati sulla scena del delitto, l'FBI introdusse i dati relativi a questi campioni nella banca dati CODIS per vedere se era possibile trovare una corrispondenza, ma il risultato della ricerca fu negativo.

Sei mesi dopo, nel novembre 1999, il profilo genetico dello sconosciuto donatore del sangue ritrovato sul luogo del crimine fu mandato al dipartimento di medicina legale dello Stato della Virginia, dove fu confrontato con i profili di 101.905 criminali archiviati nella sua banca dati. Questa volta fu trovata una corrispondenza,

la quale però riguardava soltanto otto dei tredici loci del sistema CODIS, in quanto la banca dati della Virginia, essendo più vecchia, archiviava i profili solo sulla base di quegli otto loci.

La corrispondenza di otto loci era con un uomo che figurava nell'archivio sotto il nome di Robert P. Garrett. Una ricerca tra i verbali della polizia rivelò che Robert P. Garrett era uno pseudonimo usato da un afroamericano di nome Raymond Anthony Jenkins. Questi stava scontando una pena in prigione per furto, una sentenza che era stata emanata in seguito al suo arresto nel luglio 1999, poche settimane dopo l'uccisione di Dolinger. Da quel momento in poi, le indagini della polizia si concentrarono unicamente su Jenkins.

Il 18 novembre 1999 la polizia interrogò un testimone - un uomo all'epoca sotto custodia cautelare con diverse cause pendenti - il quale sosteneva di conoscere Jenkins. Questi riferì che il giorno dopo la morte di Dolinger aveva visto Jenkins con diversi gioielli, compreso un anello di diamanti e qualche catenina d'oro, e più di mille dollari in contanti. In base a quanto riportato dai documenti ufficiali, pare anche che Jenkins avesse diversi graffi o tagli sul volto.

Sette giorni dopo la polizia eseguì un mandato di perquisizione che comprendeva il prelievo di alcuni campioni di sangue di Jenkins. Questi furono mandati al laboratorio di medicina legale dell'FBI per un confronto. Alla fine di dicembre 1999, il DNA di Jenkins fu analizzato nei tredici loci del sistema CODIS, gli otto usati dalle autorità della Virginia più altri cinque. Secondo una dichiarazione della polizia, il profilo risultante fu «positivamente identificato come corrispondente a quello delle anonime tracce di sangue ritrovate nel luogo dell'omicidio». L'analisi dell'FBI identificò il sangue di Jenkins su un paio di jeans trovati nel seminterrato vicino al corpo di Dolinger, su una maglietta nella sala da ginnastica al piano superiore, su un asciugamano appeso nel bagno del seminterrato, sul tappo del lavandino nello stesso bagno e su un corrimano tra il primo e il secondo piano della casa. L'FBI stimò che la probabilità che una persona presa a caso nella popolazione afroamericana potesse avere lo stesso profilo di Jenkins era uno su 26 quintilioni (uno su 26 miliardi di miliardi). Sulla base di quell'informazione fu emanato un mandato d'arresto e il 13 gennaio 2000 Jenkins fu arrestato.

Nell'aprile del 2000, Raymond Jenkins fu ufficialmente accusato di omicidio volontario con possesso di un'arma proibita, un'accusa che nell'ottobre dello stesso anno fu sostituita con due imputazioni di omicidio conseguente ad altro delitto, più un'imputazione di ognuno dei seguenti crimini: omicidio volontario con premeditazione, furto aggravato con uso d'armi e violenza, tentata rapina a mano armata e possesso di arma proibita.

Tale è il potere del profilo genetico, una delle armi più efficaci nell'arsenale della polizia. Tuttavia, come vedremo, quel potere poggia sulla matematica tanto quanto sulla biochimica, e non è ottenuto senza qualche costo.

La matematica del profilo genetico

A titolo di esempio introduttivo, prendiamo in considerazione un profilo basato soltanto su tre loci. La probabilità che qualcuno presenti una corrispondenza con un campione di DNA preso a caso in qualunque locus è più o meno uno su dieci (1/10).¹⁴ Pertanto, la probabilità che qualcuno presenti una corrispondenza con un campione casuale in tre loci sarebbe circa uno su mille:

$$1/10 \times 1/10 \times 1/10 = 1/1000$$

Applicando lo stesso calcolo delle probabilità a tutti i tredici loci usati nel sistema CODIS dell'FBI, otteniamo che la probabilità che qualcuno presenti una corrispondenza con un dato campione di DNA preso a caso nella popolazione è circa uno su diecimila miliardi:

$$(1/10)^{13} = 1/10.000.000.000.000$$

Questo numero è noto come probabilità di corrispondenza casuale (RMP, *Random Match Probability*). Esso viene calcolato utilizzando la regola del prodotto per moltiplicare le probabilità, che è valida soltanto se gli schemi rilevati in due loci distinti sono indipendenti. Quando furono sperimentati i primi metodi di identificazione sulla base del DNA, questo fatto diede origine ad alcuni dibattiti, ma per la maggior parte la questione sembra oggi risolta, sebbene non del tutto.

In pratica, le probabilità effettive variano, in base a diversi fattori, ma i numeri calcolati sopra sono generalmente considerati un indicatore abbastanza buono della probabilità di una corrispondenza casuale. In altre parole, la RMP viene ammessa come un buon indice della rarità di un determinato profilo genetico nella popolazione su larga scala, per quanto questa interpretazione debba essere valutata con cura (ad esempio, i gemelli identici possiedono profili genetici pressoché uguali).

Il denominatore del numero che l'FBI sosteneva di aver calcolato nel caso Jenkins (26 quintilioni) sembra spropositatamente grande, e davvero di un valore poco più che teorico, se si considera la probabilità di altri errori, come errori nell'immissione dei dati, errori di contaminazione durante la raccolta dei campioni, o errori durante il processo di analisi in laboratorio.

Nondimeno, qualunque sia il numero effettivo calcolato, non ci sono dubbi sul fatto che una corrispondenza tra profili genetici rilevata in tutti i tredici loci usati dall'FBI costituisce un'identificazione praticamente certa, *ammesso che la corrispondenza sia stata ottenuta mediante un processo che non violi il principio di casualità alla base della RMP*. Come vedremo, però, la matematica è molto sensibile alla misura in cui tale assunto viene soddisfatto.

¹⁴ Le probabilità di corrispondenza tra profili si basano su studi empirici delle frequenze alleliche in grandi numeri di campioni. La probabilità di 1/10 usata qui è comunemente considerata un buon numero rappresentativo.

Utilizzare il profilo genetico

Supponiamo che, come spesso accade, le autorità che indagano su un reato ottengano prove che indicano che il criminale potrebbe essere un certo individuo, ma non riescano a identificare il sospetto con sufficiente certezza da ottenere una condanna. Se il profilo genetico del sospetto si trova nella banca dati CODIS, o se viene prelevato un campione del suo DNA e preparato un profilo, esso potrebbe essere confrontato con quello di un campione raccolto sulla scena del delitto. Se i due profili coincidono in ognuno dei tredici loci, allora, a tutti i fini pratici e legali, si può dire che il sospetto è stato identificato con certezza. La probabilità di corrispondenza casuale (uno su diecimila miliardi) fornisce una stima affidabile della probabilità che i due profili provengano da individui diversi. (L'unica clausola è che vengano esclusi i parenti. Ciò non è sempre facile, nemmeno nel caso di parenti stretti come fratelli e sorelle; infatti, talvolta, un individuo potrebbe non sapere di avere un fratello o una sorella da cui è stato separato alla nascita, e i documenti ufficiali non sempre corrispondono alla realtà.)

Naturalmente, tutto quello che una corrispondenza di profili genetici può fare è identificare - entro un certo grado di certezza - un individuo il cui profilo genetico è uguale a quello di uno o più campioni ritrovati sulla scena del delitto. Ciò non implica che sia stato quell'individuo a commettere il reato. Per arrivare a questa conclusione occorrono altre prove. Ad esempio, se lo sperma prelevato dalla vagina di una donna che è stata violentata e uccisa rivela una corrispondenza di profilo genetico con un certo individuo, allora, entro il grado di accuratezza calcolato per la procedura, si può assumere che l'individuo abbia avuto un rapporto sessuale con la donna poco prima della sua morte. Sarebbero però necessarie altre prove per concludere che l'uomo ha violentato la donna, e forse altre ancora per dimostrare che è stato lui a ucciderla. Una corrispondenza di DNA è soltanto quello che è: una corrispondenza di due profili.

Quanto al grado di certezza che si può attribuire all'identificazione di un individuo per mezzo di una corrispondenza di profili genetici ottenuta nella maniera descritta sopra, i punti da considerare sono:

- la probabilità di errori nel processo di raccolta e classificazione dei due campioni e di determinazione dei relativi profili genetici;
- la probabilità che la corrispondenza tra i due profili sia una pura coincidenza.¹⁵

Una probabilità di uno su diecimila miliardi annessa alla seconda di queste due possibilità (così come è data dalla RMP per una corrispondenza in tredici loci) implicherebbe chiaramente che la prima possibilità è molto più probabile, essendo difficile che qualche procedura umana possa rivendicare una frequenza di errore di uno su diecimila miliardi. In altre parole, se non c'è ragione di dubitare dell'accuratezza delle procedure di raccolta dei campioni e delle analisi di

¹⁵ Come spiegheremo più avanti, bisogna fare attenzione a interpretare questo requisito nei termini dell'esatta probabilità numerica che deve essere calcolata.

laboratorio, l'identificazione basata sul profilo genetico potrebbe sicuramente essere considerata attendibile, con un alto grado di certezza. Questo però vale soltanto se la corrispondenza è stata ottenuta confrontando il profilo di un campione prelevato dalla scena del delitto con quello di un sospetto *che è già stato identificato mediante prove diverse dal suo profilo genetico*. Ma nel caso di Jenkins le cose andarono altrimenti. Egli divenne un indiziato soltanto perché gli investigatori passarono al setaccio una banca dati di profili genetici (a dire il vero, due banche dati) finché non trovarono una corrispondenza: una procedura nota con il nome di «colpo a freddo» (*cold hit*). Questo ci porta a calcoli matematici completamente diversi.

I rischi del colpo a freddo

In genere, una ricerca in una banca dati di DNA condotta per vedere se si riesce a trovare un profilo che corrisponde a quello di un dato campione - poniamo, uno raccolto sul luogo di un crimine - viene chiamata «ricerca del colpo a freddo» (*cold hit search*). Una corrispondenza di profili genetici risultante da una ricerca siffatta viene definita «a freddo» perché prima che tale corrispondenza venisse trovata l'individuo interessato non era un sospetto.

Ad esempio, il sistema CODIS consente ai laboratori di polizia scientifica a livello statale e locale di condurre ricerche che potrebbero rivelare che lo sperma depositato durante un caso irrisolto di stupro in Florida ha un profilo genetico coincidente con quello di un noto criminale della Virginia.

Come nel caso in cui il profilo del DNA è impiegato per identificare un individuo già sospettato, la domanda fondamentale che occorrerebbe porsi dopo aver ottenuto una corrispondenza a freddo è: la corrispondenza indica che il profilo contenuto nella banca dati appartiene alla stessa persona il cui campione ha costituito la base della ricerca, o è una pura coincidenza? A questo punto, le acque matematiche diventano inaspettatamente torbide.

Per illustrare i problemi intrinseci al colpo a freddo, consideriamo la seguente analogia. In una tipica lotteria nazionale, la probabilità di vincere un grosso montepremi è circa uno su trentacinque milioni. Per ogni singolo individuo, comprare il biglietto è chiaramente una perdita di tempo. Le probabilità sono effettivamente irrisorie. Ma supponiamo che ogni settimana almeno trentacinque milioni di persone comprino davvero un biglietto (questo è un esempio realistico). Allora, in media, ogni una, due o tre settimane, qualcuno vincerà e i giornalisti andranno a intervistare il fortunato. Che cos'ha di speciale questa persona? Assolutamente niente. L'unica cosa che possiamo dire di lui o di lei è che è la persona che aveva i numeri vincenti. Non possiamo trarre nessun'altra conclusione. La probabilità di uno su trentacinque milioni non suggerisce nessun'altra caratteristica di quella persona. Il fatto che ci sia un vincitore è un riflesso del fatto che trentacinque milioni di persone hanno comprato un biglietto, e niente più.

Confrontiamo questo caso con quello in cui un giornalista sente dire che una certa persona ha la reputazione di essere molto fortunata, la accompagna a comprare il biglietto e le siede vicino mentre ascolta i risultati della lotteria annunciati in

televisione. E, guarda caso, la persona vince! Che cosa potremmo concludere? Molto probabilmente, che si tratta di una truffa. Con una probabilità di uno su trentacinque milioni, è impossibile concludere qualcos'altro in questa situazione.

Nel primo caso, la bassa probabilità non ci dice nulla sulla persona che ha vinto, a parte il fatto che ha vinto. Nel secondo caso, la bassa probabilità ci dice molto.

Un colpo a freddo misurato dalla RMP è come il primo caso. Ci dice soltanto che c'è una corrispondenza di profili genetici. Di per sé, non ci dice nient'altro, e sicuramente non ci dice che la persona in questione è colpevole del crimine.

D'altro canto, se un individuo viene identificato come sospetto di un reato attraverso prove diverse da una coincidenza di profili genetici, allora una corrispondenza di DNA trovata in seguito è analoga al secondo caso. Ci dice molto. In questo caso, posto che l'identificazione iniziale avesse una base ragionevole e significativa (come la reputazione di essere fortunato nel caso della lotteria), la bassa probabilità di una corrispondenza casuale potrebbe essere considerata una prova decisiva. Ma, come nell'esempio della lotteria, perché la bassa probabilità abbia qualche valore l'identificazione iniziale deve *avvenire prima* che sia effettuato il confronto dei profili genetici (o, per lo meno, deve essere chiaramente indipendente da questo). Se il confronto dei profili genetici viene effettuato prima, quella probabilità incredibilmente bassa potrebbe non avere alcun significato.

I rapporti NRC I e NRC II

Nel 1989, mossa dal desiderio di sfruttare le nuove tecnologie emergenti per l'identificazione dei sospetti nei casi di crimine sulla base del profilo genetico, comprese le identificazioni a freddo, l'FBI esortò il National Research Council a condurre uno studio sulla materia. L'NRC costituì un Committee on DNA Technology in Forensic Science, una commissione d'inchiesta sulle tecnologie genetiche in medicina legale, che pubblicò il suo rapporto nel 1992. Intitolato *DNA Technology in Forensic Science* e pubblicato da National Academy Press, il rapporto viene spesso citato con la sigla NRC I. La principale raccomandazione della commissione in merito alle identificazioni basate su corrispondenze a freddo era:

La differenza tra scoprire che un campione ritrovato sulla scena di un crimine corrisponde a uno prelevato da un sospetto e scoprire che un campione raccolto sul luogo del reato corrisponde a uno dei molti profili genetici archiviati in una banca dati è importante. La probabilità di trovare una corrispondenza nel secondo caso è assai più elevata [...] La corrispondenza iniziale dovrebbe essere considerata un buon motivo per ottenere un nuovo campione di sangue dal sospetto, ma solo la frequenza statistica associata ai nuovi loci esaminati dovrebbe essere presentata in tribunale (per prevenire le distorsioni nel processo di selezione che sono intrinseche alle ricerche in una banca dati).

In parte a causa delle controversie che il rapporto NRC I generò tra gli scienziati in merito alla metodologia proposta, e in parte perché i tribunali spesso fraintesero o applicarono male alcune delle affermazioni contenute nel rapporto, nel 1993 l'NRC condusse un nuovo studio. Fu costituita una seconda commissione, che pubblicò il

suo rapporto nel 1996. Spesso citato con la sigla NRC II, il secondo rapporto, dal titolo *The Evaluation of Forensic DNA Evidence*, fu pubblicato da National Academy Press nel 1996. Questa volta, la principale raccomandazione della commissione in merito alle probabilità di false identificazioni nei casi di corrispondenze a freddo era:

Quando il sospetto viene trovato per mezzo di una ricerca in una banca dati di DNA, la probabilità di corrispondenza casuale dovrebbe essere moltiplicata per N, il numero delle persone contenute nella banca dati.

La regola statistica raccomandata dal rapporto NRC II viene generalmente chiamata «probabilità di corrispondenza in una banca dati», o DMP (*Database Match Probability*). La scelta del nome è poco azzeccata, dal momento che la DMP *non* è una probabilità, anche se in tutti i casi reali essa è di fatto un numero compreso tra 0 che fornisce (a parere della seconda commissione dell'NRC) una buona indicazione della probabilità di ottenere una corrispondenza accidentale quando viene condotta una ricerca in una banca dati. (L'intuizione alla base della regola è piuttosto chiara: quando si cerca una corrispondenza in una banca di N dati, ci sono N possibilità di trovare una simile corrispondenza.) Per una vera misura di probabilità, se un evento ha probabilità 1, allora è certo che si verificherà. Ma consideriamo un caso ipotetico in cui viene esaminata una banca di un milione di dati per cercare un profilo avente una RMP di 1/1.000.000. In questo caso, la DMP sarà:

$$1.000.000 \times 1/1.000.000 = 1$$

Tuttavia, in questo caso, la probabilità di trovare una corrispondenza non è 1 ma circa 0,6312.

La spiegazione fornita dalla commissione delle ragioni per raccomandare l'uso della DMP come misura scientifica dell'accuratezza di una corrispondenza a freddo è la seguente:

Si crea una circostanza speciale quando il sospetto viene identificato non da un testimone oculare o da prove circostanziali ma da una ricerca condotta in una vasta banca dati di DNA. Se l'unica ragione per cui la persona diviene un sospetto è che il suo profilo genetico è stato trovato in una banca dati, i calcoli devono essere modificati. Dei diversi metodi esistenti ne prendiamo in esame due. Il primo, difeso dal rapporto dell'NRC del 1992, consiste nel basare il calcolo delle probabilità unicamente sui loci che non sono stati utilizzati nella ricerca. Tale procedura è sensata, ma spreca informazioni, e se vengono usati troppi loci per l'identificazione del sospetto, potrebbero non rimanerne abbastanza per un'adeguata analisi successiva [...] Una seconda procedura consiste nell'applicare una semplice correzione: moltiplicare la probabilità di corrispondenza per le dimensioni della banca dati esaminata. Questo è il metodo che raccomandiamo.

Questa è essenzialmente la stessa logica del nostro paragone con la lotteria. Nel caso Jenkins, la DMP associata all'originaria ricerca nella banca dati della Virginia (contenente 101.905 profili archiviati sulla base di otto loci) sarebbe approssimativamente:

$$100.000 \times 1/100.000.000 = 1/1000$$

Con un simile valore, la probabilità di una corrispondenza accidentale in una ricerca a freddo condotta in una banca dati di DNA è piuttosto alta (ricordiamo il paragone con la lotteria). Così, quello che sembrava a prima vista un caso inequivocabile improvvisamente comincia ad apparire meno chiaro. Questo è ciò che pensano anche i tribunali. Nel momento in cui scriviamo, il caso Jenkins è ancora aperto ed è diventato una delle molte cause legali negli Stati Uniti che vengono studiate come modello per altri casi analoghi.

Numeri in tribunale: le opzioni statistiche

Finora, i tribunali si sono dimostrati restii all'idea che le giurie siano messe di fronte alle argomentazioni statistiche riguardanti casi di corrispondenza a freddo dei profili genetici. Tale posizione è ragionevole. Fino a oggi, gli esperti hanno proposto almeno cinque procedure diverse per calcolare la probabilità che un'identificazione a freddo produca un falso risultato, vale a dire che identifichi qualcuno che, per puro caso, ha lo stesso profilo genetico del campione ritrovato sulla scena del delitto. I cinque metodi sono:

1. *Riferire solo la RMP.* Sebbene alcuni statistici abbiano argomentato a favore di questo approccio, altri lo hanno fortemente criticato. Il rapporto NRC II si pronunciò fermamente contro qualsiasi menzione della RMP in tribunale.
2. *Riferire solo la DMP.* Questo è l'approccio difeso dal rapporto NRC II.
3. *Riferire sia la RMP sia la DMP.* Tale approccio è difeso dal DNA Advisory Board dell'FBI, il quale ritiene che entrambe le stime siano «di particolare interesse» per la giuria in un caso di identificazione a freddo, sebbene non sia chiaro come persone non esperte potrebbero apprezzare il significato relativo dei due valori. E non è nemmeno chiaro perché dovremmo chieder loro di farlo, considerato che alcuni dei più grandi statistici del mondo sembrano in disaccordo sulla questione.
4. *Riferire i risultati di un'analisi bayesiana alternativa.* Alcuni statistici sostengono che il problema di assegnare una probabilità a un'identificazione a freddo dovrebbe essere affrontato da una prospettiva bayesiana. (Per una trattazione della statistica bayesiana si rimanda al capitolo 6.) Utilizzando l'analisi bayesiana per calcolare una stima statistica dell'attendibilità di una corrispondenza a freddo, si ottiene un numero solo leggermente più piccolo della RMP.
5. *Riferire la RMP calcolata sui loci di conferma non considerati nella ricerca iniziale.* Questo è l'approccio difeso dal rapporto NRC I.

A questo punto, un profano potrebbe dire: «Allora, siccome l'identificazione basata sul profilo genetico ha una frequenza di errore inferiore a uno su molte migliaia di miliardi, la probabilità di ottenere una falsa corrispondenza in una banca

di, poniamo, tre milioni di dati, come il sistema CODIS, è così bassa che, indipendentemente da quale metodo venga usato per calcolare le probabilità, una corrispondenza potrà essere sicuramente considerata una prova definitiva». L'idea che sta dietro a una simile conclusione è presumibilmente questa: effettuando una ricerca nella banca dati ci sono tre milioni di possibilità di trovare una corrispondenza; pertanto se la probabilità di corrispondenza casuale è 1 su 10.000.000.000.000, la probabilità di trovare una corrispondenza in tutta la banca dati è circa 1 su 3.000.000 (3.000.000 diviso per 10.000.000.000.000 fa circa 1/3.000.000).

Purtroppo - almeno per lo sfortunato innocente cui può capitare di divenire un sospetto in questo modo - tale argomentazione non è valida. Infatti, indipendentemente dal fatto che la RMP sia dell'ordine di «uno su molte migliaia di miliardi», persino una banca dati di DNA piuttosto piccola ha una buona probabilità di contenere diverse coppie di profili genetici che combaciano per puro caso. Una bassa RMP non significa che non possano esserci corrispondenze casuali. Questa è una versione più sottile del famoso problema del compleanno, secondo il quale è sufficiente radunare in una stanza 23 persone scelte a caso perché ci sia una probabilità superiore al cinquanta per cento che due di esse compiano gli anni lo stesso giorno. (Il calcolo preciso è un po' complesso, ma possiamo farcene un'idea se consideriamo che con 23 persone ci sono $23 \times 22 = 506$ coppie possibili, ognuna delle quali potrebbe essere composta da due individui che compiono gli anni lo stesso giorno, e che questo numero di coppie risulta sufficiente a far sì che la probabilità di trovare una corrispondenza divenga pari a 0,508.)

Ad esempio, la banca dati di DNA dei prigionieri dell'Arizona, contenente circa 65.000 profili realizzati sulla base di tredici loci, è piuttosto piccola. Supponiamo, per semplicità, che la probabilità di una corrispondenza casuale per un singolo locus sia pari a 1/10, un numero che, come abbiamo osservato prima, risulta piuttosto ragionevole. Pertanto, la RMP per nove loci sarà $1/10^9$, vale a dire uno su un miliardo. Si potrebbe pensare che, data questa bassissima probabilità che due profili presi a caso corrispondano in nove loci, è altamente improbabile che la banca dati contenga una coppia di profili identici per questi nove loci. Eppure, in virtù di un ragionamento simile a quello usato nel problema del compleanno, la probabilità di trovare due profili coincidenti in nove loci è circa del cinque per cento, o uno su venti. Per una banca di 65.000 dati, ciò significa che c'è una buona probabilità di trovare alcuni profili corrispondenti!

Illustreremo schematicamente i calcoli alla fine del capitolo, ma la risposta diventa meno sorprendente se si considera che in una banca di 65.000 dati ci sono all'incirca 65.000^2 - ovvero 4.225.000.000 - coppie possibili, ognuna delle quali potrebbe essere composta da due profili coincidenti in nove loci.

Infatti, nel 2005 un'analisi condotta sulla banca dati dell'Arizona rivelò che 144 individui avevano profili genetici corrispondenti in nove loci. Un altro piccolo gruppo presentava una corrispondenza in dieci loci, due profili coincidevano in undici loci e altri due avevano dodici loci identici. Si scoprì che gli individui con undici e dodici loci identici erano fratelli, fatto che indicava una corrispondenza non casuale. Ma tutti gli altri non lo erano, e quei risultati erano di fatto vicini a quello

che ci si aspetterebbe dai calcoli matematici se sostituissimo la probabilità di 1/10 che abbiamo assunto per la corrispondenza in un singolo locus con un valore realistico ottenuto empiricamente.

Tutto questo si traduce in un incubo matematico per i giudici e per le giurie che devono emettere un verdetto in tribunale. Tuttavia, anche tenendo in considerazione tutte le complicazioni matematiche, l'identificazione sulla base del profilo genetico è assai più affidabile della tecnica molto più vecchia delle impronte digitali, che esamineremo nel capitolo 9.

Il calcolo della probabilità di una corrispondenza in una banca dati

Presentiamo qui i calcoli cui abbiamo accennato prima. Ricordiamo che abbiamo una banca dati di profili genetici contenente 65.000 profili realizzati su tredici loci. Supponiamo che la probabilità di una corrispondenza casuale in un singolo locus sia pari a 1/10, e che la RMP per una corrispondenza in nove loci sia quindi uguale a $1/10^9$, ovvero uno su un miliardo.

Ora, ci sono $13!/[9! \times 4!] = [13 \times 12 \times 11 \times 10]/[4 \times 3 \times 2 \times 1] = 715$ modi possibili di scegliere nove di tredici loci, così che la probabilità di trovare una corrispondenza casuale in *qualunque* gruppo di nove dei tredici loci è $715/10^9$.

Se si prende un profilo qualsiasi nella banca dati, la probabilità che un secondo profilo non corrisponda a quello in nove loci è $1 - 715/10^9$.

Pertanto, la probabilità che tutti i 65.000 profili della banca dati non corrispondano in *nove* loci è all'incirca $(1 - 715/10^9)^{65000}$. Usando il teorema del binomio, ciò equivale approssimativamente a $1 - 65.000 \times 715/10^9 = 1 - 46.475/10^6$, ovvero circa a $1 - 0,05$.

La probabilità che ci sia una corrispondenza in nove loci è data dalla differenza tra 1 e questo numero, ovvero $1 - (1 - 0,05) = 0,05$.

SEGRETI: CREARE E DECIFRARE I CODICI

L'ipotesi di Riemann

Nel quinto episodio della prima serie di *NUMB3RS*, mandato in onda in Italia con il titolo *L'ipotesi di Riemann* il 10 giugno 2007, una bambina di cinque anni viene rapita. Don chiede l'aiuto di Charlie quando scopre che anche il padre della bambina, Ethan, è un matematico. Quando Charlie vede i calcoli che Ethan ha scribacchiato sulla lavagna bianca nel suo studio, capisce che sta lavorando all'ipotesi di Riemann, un famoso problema di matematica che da oltre centocinquant'anni resiste a ogni tentativo di risolverlo.

Il problema di Riemann è uno dei cosiddetti «problemi del millennio», una lista di enigmi matematici irrisolti stilata da un panel internazionale di esperti nel 2000, per ognuno dei quali è stato istituito un premio di un milione di dollari destinato a chi dovesse riuscire a risolverlo. Nel caso del problema di Riemann, probabilmente una soluzione non porterebbe soltanto a un premio di un milione di dollari, ma a qualcosa in più. Essa potrebbe infatti implicare un grosso progresso negli studi su come fare a scomporre grandi numeri in numeri primi, e così fornire un metodo per decifrare i codici di sicurezza utilizzati per criptare le comunicazioni via Internet. Se dovesse accadere una cosa del genere, il commercio via Internet andrebbe immediatamente in rovina, generando enormi conseguenze sul piano economico.

Quando Don riesce a scoprire l'identità di uno dei rapitori e viene a sapere che il piano è di «svelare il più grosso segreto economico del mondo» capisce chiaramente perché la figlia di Ethan è stata rapita. I rapitori vogliono usare il metodo di Ethan per entrare nel computer di una banca e rubare milioni di dollari. Per Don, la strategia più ovvia è che Ethan fornisca alla banda la chiave per entrare nel computer della banca in modo da poter tracciare l'attività elettronicamente al fine di catturare i ladri. Ma quando Charlie trova un grosso errore nel ragionamento di Ethan, l'unica speranza che rimane a Don di poter salvare sua figlia è di escogitare un modo per far credere ai rapitori che egli è davvero in grado di fornire la chiave di criptaggio in Internet che richiedono, per poi risalire al luogo in cui tengono prigioniera la bambina.

A un certo punto dell'episodio, Charlie tiene una lezione agli agenti dell'FBI su come il criptaggio in Internet dipenda dalla difficoltà di scomporre grandi numeri in numeri primi. In un'altra scena dell'episodio, Charlie ed Ethan discutono della possibilità di tradurre la soluzione di Ethan in un algoritmo e Charlie fa riferimento all'«espansione della regione priva di zeri verso la linea critica». Charlie osserva anche che i rapitori, per scomporre un grande numero in numeri primi, avrebbero bisogno di un supercomputer. La sua studentessa Amita fa notare che è possibile costruire un supercomputer collegando tra loro tanti computer. Come sempre, queste sono tutte affermazioni matematicamente sensate e realistiche. Vale lo stesso per la

premessa fondamentale della storia: una soluzione del problema di Riemann potrebbe effettivamente portare al collasso dei metodi attualmente utilizzati per mantenere sicure le comunicazioni in Internet. A partire dalla Seconda guerra mondiale, il criptaggio dei messaggi è sempre stato un compito dei matematici.

www.cybercrime.gov

Oggigiorno, non occorre una pistola o un coltello per rubare denaro. Sono sufficienti un personal computer da pochi soldi e una connessione a Internet. Si chiama crimine informatico, una nuova forma di crimine molto diffusa e in continua crescita. Il termine comprende un'ampia gamma di attività illegali, quali pirateria software, pirateria musicale, frode con le carte di credito (di vario tipo), furto di identità, manipolazione di titoli, spionaggio aziendale, pornografia infantile e *phishing* (che consiste nel mandare a un utente di computer una mail che, fingendo di provenire da qualche organismo finanziario, cerca di indurre con l'inganno il ricevente a rivelare le sue coordinate bancarie e altri dati personali).

Non esistono stime affidabili sull'estensione del crimine informatico, giacché molte banche e varie compagnie di commercio in Internet tengono segrete queste informazioni per non dare l'impressione che il vostro denaro o il numero della vostra carta di credito non siano sicuri nelle loro mani. E' stato suggerito, sebbene la cosa sia oggetto di accese dispute, che i proventi annuali del crimine informatico ammontino a oltre cento miliardi di dollari. Se fosse vero, la cifra supererebbe quella delle vendite di droghe illegali. Indipendentemente dai numeri effettivi, il crimine informatico è un problema abbastanza grosso da aver indotto sia il dipartimento della Giustizia degli Stati Uniti sia l'FBI a dedicare interi reparti alla lotta contro queste attività criminali e a creare ciascuno il proprio sito Internet informativo sulla questione: www.cybercrime.gov e <http://www.fbi.gov/cyberinvest/cyberhome.htm> rispettivamente.

Il rilevamento sulla criminalità informatica realizzato dall'FBI nel 2005 con l'aiuto delle principali autorità pubbliche e private sulla sicurezza informatica, e basato sulle risposte fornite da un campione trasversale di più di duemila organizzazioni pubbliche e private in quattro Stati, riferì che:

- circa nove organizzazioni su dieci hanno sperimentato violazioni della sicurezza informatica durante l'anno; il 20 per cento di queste organizzazioni ha dichiarato di aver subito venti o più attacchi; virus (83,7 per cento) e spyware (79,5 per cento) erano in cima alla lista;
- più del 64 per cento dei rispondenti ha subito una perdita economica. I principali responsabili indicati sono virus e *worms*, cui si deve una perdita di 12 milioni di dollari sui 32 milioni di dollari totali;
- gli attacchi provengono da 36 nazioni diverse. Gli Stati Uniti (26,1 per cento) e la Cina (23,9 per cento) erano all'origine di più della metà dei tentativi di intrusione, anche se il fatto che molti trasgressori operino attraverso uno o più computer intermedi in diversi Paesi rende difficile ottenere stime accurate.

Gli agenti di polizia che concentrano le loro energie nella lotta contro il crimine informatico fanno spesso uso della matematica. In molti casi, essi impiegano le stesse tecniche che abbiamo descritto in altri punti del libro. In questo capitolo, tuttavia, rivolgeremo la nostra attenzione a un'importante area della lotta contro il crimine informatico che si serve di differenti metodi matematici, ovvero la sicurezza in Internet. In questo campo, l'uso ingegnoso di alcune sofisticate tecniche matematiche ha portato a considerevoli progressi, con il risultato che, se propriamente usati, i sistemi oggi a disposizione per mantenere sicure le comunicazioni via Internet sono estremamente affidabili.

Mantenere i segreti

Se usate un bancomat per prelevare denaro dal vostro conto corrente, o mandate i dettagli della vostra carta di credito a un rivenditore in Internet, vorrete esser sicuri che soltanto il destinatario cui intendete mandare i vostri dati abbia accesso a queste informazioni. Ciò non può essere fatto impedendo a qualche terzo non autorizzato di «intercettare» i messaggi elettronici che state scambiando con l'organizzazione interessata. Internet è ciò che viene chiamato un sistema aperto, il che significa che le connessioni tra i milioni di computer che formano la rete sono, a tutti gli effetti, pubbliche. La sicurezza del traffico di comunicazioni in Internet è raggiunta per mezzo del criptaggio, una tecnica che permette di «codificare» i messaggi in modo che, anche se qualcuno non autorizzato intercetta il segnale trasmesso, non sarà in grado di decifrarlo.

Il concetto di criptaggio non è nuovo. L'idea di usare un codice segreto per occultare il contenuto di un messaggio risale almeno ai tempi dell'Impero romano, quando Giulio Cesare faceva uso di codici segreti per garantire la sicurezza degli ordini che mandava ai suoi generali durante le guerre galliche. In quello che è oggi chiamato cifrario di Cesare, il messaggio originale viene trasformato prendendo a turno ogni lettera di ciascuna parola e sostituendola con un'altra lettera in base a qualche regola fissa, ad esempio sostituendo ogni lettera con quella che si trova tre posizioni più avanti nell'alfabeto: la A viene sostituita dalla D, la G dalla J, la Z dalla C e così via. Con questo codice, la parola «matematica» diventerebbe «pdwhpdwlfd».

Un messaggio criptato utilizzando un cifrario di Cesare potrebbe sembrare a prima vista del tutto indecifrabile senza conoscere la regola usata, ma non è affatto così. Intanto, nell'alfabeto internazionale esistono soltanto venticinque cifrari a sostituzione monoalfabetica di questo tipo, e un nemico che sospettasse che ne state utilizzando uno non dovrebbe fare altro che provarli tutti fino a trovare quello giusto.

Un metodo un po' più efficace consisterebbe nell'impiegare qualche altra regola, meno ovvia, per sostituire le lettere. Purtroppo, però, qualunque codice del genere, che si limita a sostituire una lettera con un'altra, può essere decifrato facilmente con una semplice analisi degli schemi di sostituzione. Ad esempio, in italiano (come in qualunque altra lingua) le singole lettere ricorrono con frequenze ben definite, e

contando il numero di occorrenze di ogni lettera nel vostro testo cifrato un nemico potrà facilmente dedurre qual è la regola di sostituzione che avete utilizzato, specialmente se fa uso di un computer per accelerare il processo.

Accantonando la sostituzione semplice, quale altro metodo si potrebbe provare? Qualunque cosa scegliate, i rischi sono più o meno gli stessi. Se il vostro testo cifrato contiene qualche schema riconoscibile, una sofisticata analisi statistica può solitamente decifrarlo senza grosse difficoltà.

Per essere sicuro, quindi, un sistema di criptaggio deve distruggere qualunque schema che, se scoperto, potrebbe consentire al nemico di decifrare il codice. Tuttavia, la trasformazione del messaggio eseguita tramite un sistema di criptaggio chiaramente non può distruggere *ogni* ordine: dietro a tutto questo il messaggio deve esistere ancora affinché il destinatario possa recuperarlo. Il trucco, quindi, è di progettare il sistema di criptaggio in modo che questo ordine nascosto sia sepolto abbastanza in profondità da impedire a un eventuale nemico di scoprirlo.

Tutti i sistemi cifrati impiegati a partire dalla fine della Seconda guerra mondiale si basano sulla matematica e sull'uso di computer. Questa è una necessità, in quanto tali sistemi devono essere abbastanza complessi da resistere a eventuali attacchi informatici sferrati da nemici dotati di computer potenti.

Occorre molto tempo e molto lavoro per progettare e creare un sistema di criptaggio sicuro. Per evitare di dover continuare a creare nuovi sistemi, i moderni sistemi di criptaggio consistono sempre di due componenti: una procedura di criptaggio e una «chiave». La prima è, solitamente, un programma informatico o, in certi casi, un computer specificamente progettato. Per criptare un messaggio il sistema necessita non solo del messaggio in questione, ma anche della chiave scelta, generalmente un numero segreto. Il programma di criptaggio codificherà il messaggio in un modo che dipende dalla chiave scelta, così che solo conoscendo quella chiave sarà possibile decodificare il testo cifrato. Dato che la sicurezza dipende dalla chiave, lo stesso programma di criptaggio può essere utilizzato da diverse persone per molto tempo, e ciò significa che la sua progettazione può richiedere una grande quantità di tempo e di lavoro.

Un'ovvia analogia è con i costruttori di casseforti e serrature. Questi, infatti, possono mandare avanti la loro attività progettando un tipo di serratura che può essere venduto a centinaia di utenti, i quali, come garanzia di sicurezza, fanno affidamento sull'unicità della loro chiave (che in questo caso potrebbe essere una chiave materiale o una combinazione numerica). Proprio come un ladro potrebbe sapere come è stata progettata la serratura e non essere tuttavia in grado di aprire la vostra cassaforte senza avere la chiave materiale o conoscere la combinazione, allo stesso modo un nemico potrebbe sapere quale sistema di criptaggio state usando senza essere in grado di decifrare i vostri messaggi in codice: un'impresa per cui occorrerebbe conoscere la chiave.

In alcuni sistemi di criptaggio basati sull'uso di una chiave, il mittente e il destinatario decidono prima, di comune accordo, quale sarà la chiave segreta che utilizzeranno per scambiarsi i messaggi. Finché i due mantengono segreta questa chiave il sistema, se ben progettato, dovrebbe essere sicuro. Un meccanismo di questo tipo che è stato utilizzato per molti anni, sebbene oggi sia considerato un po'

vecchio e vulnerabile agli attacchi di nemici che impiegano computer molto più veloci di quelli disponibili all'epoca in cui fu creato, è il sistema americano Data Encryption Standard (DES). La chiave del DES richiede un numero avente una rappresentazione binaria a 56 bit (in altre parole, una sequenza di 56 zero e uno). Perché una chiave così lunga? La ragione è che al tempo in cui il sistema fu progettato nessuno mantenne segreto il suo modo di operare. Tutti i dettagli furono resi pubblici fin dall'inizio. Ciò significa che un nemico avrebbe potuto decifrare i messaggi semplicemente provando con tutte le chiavi possibili, una dopo l'altra, finché non avesse trovato quella giusta. Nel DES le chiavi da provare erano 2^{56} , un numero abbastanza grande da rendere l'impresa pressoché irrealizzabile ai tempi in cui si cominciò a usare questo sistema.

I sistemi di criptaggio come il DES hanno un evidente svantaggio. Prima che un simile schema possa essere utilizzato, il mittente e il ricevente devono mettersi d'accordo sulla chiave che useranno. Siccome vorranno sicuramente evitare di trasmettere la loro chiave su un canale di comunicazione, dovranno incontrarsi di persona, o al limite servirsi di un corriere fidato per trasferire la chiave dall'uno all'altro. Questo va bene per stabilire l'accesso via Internet al vostro conto corrente; potete semplicemente recarvi di persona alla vostra filiale locale e decidere la chiave. Ma è assolutamente inutile se si vuole istituire una comunicazione sicura tra individui che non si sono mai incontrati prima. In particolare, tale sistema non è adatto per il commercio in Internet, dove sentiamo l'esigenza di mandare messaggi sicuri da una parte all'altra del mondo a qualcuno che non abbiamo mai incontrato.

Crittografia a chiave pubblica

Nel 1976, due giovani ricercatori della Stanford University, Whitfield Diffie e Martin Hellman, pubblicarono un articolo che segnò una svolta decisiva nelle ricerche sui meccanismi di criptaggio. In questo articolo, intitolato *New Directions in Cryptography*, essi proposero un nuovo tipo di sistema: la crittografia a chiave pubblica. In un sistema a chiave pubblica, il metodo di criptaggio richiede non una ma due chiavi: una per codificare e l'altra per decodificare il messaggio (è come avere una serratura che necessita di una chiave per chiuderla e di un'altra per aprirla). Un sistema del genere, suggerivano gli autori, sarebbe utilizzato nel modo seguente.

Una persona, mettiamo si chiami Alice, che desidera servirsi del sistema acquista il programma standard (o il computer speciale) utilizzato da tutti i membri della rete di comunicazione interessata. Poi Alice genera due chiavi. Di queste due chiavi una, quella che le servirà per decifrare i messaggi, la tiene segreta. L'altra chiave invece, quella che qualunque altro membro della rete dovrà utilizzare per codificare i messaggi che vuole mandare *a lei*, la rende pubblica in una directory degli utenti della rete.

Se un altro utente della rete, mettiamo si chiami Carlo, vuole mandare un messaggio ad Alice, cerca la chiave pubblica di criptaggio di Alice, la usa per codificare il messaggio e quindi le manda il messaggio criptato. Per decodificare il

messaggio non serve a niente conoscere la chiave di criptaggio di Alice (accessibile a tutti). Occorre la chiave di decriptaggio che solo Alice, la destinataria, conosce. (Una caratteristica interessante di tale sistema è che una volta che Carlo ha codificato il messaggio non può più decodificarlo; quindi, se volesse riferirsi a esso in un momento successivo, farebbe meglio a tenere una copia della versione originale non criptata!)

Diffie e Hellman non riuscirono a fornire un metodo adeguato per costruire un sistema di questo tipo, ma l'idea era geniale e poco tempo dopo altri tre ricercatori del Massachusetts Institute of Technology (MIT), Ronal Rivest, Adi Shamir e Leonard Adleman, trovarono il modo di metterla in opera. La loro idea era di sfruttare i punti forti e deboli di quegli stessi computer la cui esistenza rende tanto difficile il lavoro di chi progetta uno schema di criptaggio.

Progettare un programma informatico capace di trovare grandi numeri primi, diciamo dell'ordine delle 150 cifre, risulta relativamente semplice. È anche facile moltiplicare tra loro due grandi numeri primi di questo tipo per produrre un unico numero (composto) di 300 cifre o più. Ma scomporre un numero di quelle dimensioni in fattori primi non è affatto semplice e in realtà è, a tutti gli effetti, impossibile (più precisamente, anche il computer più veloce del mondo impiegherebbe molti decenni, o addirittura secoli, per trovare questi fattori). Il sistema a chiave pubblica basato su questa idea è chiamato sistema RSA, dalle iniziali dei nomi dei suoi tre inventori. Il successo del metodo portò alla fondazione di una società commerciale specializzata nella sicurezza dei dati: la RSA Data Security a Redwood City, in California.

La chiave di decifrazione segreta utilizzata nel metodo RSA consiste essenzialmente di due grandi numeri primi scelti dall'utente (con l'aiuto di un computer, non presi da qualche lista pubblica di numeri primi, cui un nemico potrebbe avere accesso!). La chiave di crittografia pubblica è il prodotto di questi due numeri primi. Dal momento che non è noto alcun metodo veloce per scomporre grandi numeri in fattori primi, è praticamente impossibile recuperare la chiave di decriptaggio dalla chiave pubblica di criptaggio. La codifica del messaggio corrisponde alla moltiplicazione di due grandi numeri primi (una facile operazione computazionale), mentre la decodifica corrisponde al processo opposto di scomposizione in fattori primi (una difficile operazione computazionale).

È importante puntualizzare che il criptaggio e il decriptaggio non sono in realtà ottenuti rispettivamente moltiplicando numeri primi e scomponendo i numeri in fattori primi. Piuttosto, questo è il modo in cui vengono generate le chiavi. L'espressione «corrisponde a» nella precedente descrizione dovrebbe essere letta in termini approssimativi. Ma per quanto le operazioni di codifica e decodifica non siano mere moltiplicazioni e scomposizioni in fattori primi, il sistema RSA resta un sistema aritmetico. Il messaggio viene dapprima tradotto in forma numerica e i processi di criptaggio e decriptaggio consistono di operazioni aritmetiche piuttosto semplici eseguite sui numeri.

Dunque è chiaro che la sicurezza del sistema RSA, e di conseguenza delle molte reti internazionali di dati che ne fanno uso, fa affidamento *sull'incapacità* dei matematici di trovare un metodo efficace per determinare i fattori primi dei grandi numeri.

Com'era da aspettarsi, visto quello che c'è in ballo, l'uso generalizzato del sistema RSA ha stimolato una gran quantità di ricerche sui problemi della determinazione dei numeri primi e dei fattori dei grandi numeri.

Il modo più ovvio per stabilire se un numero N è primo oppure no è vedere se è divisibile per un numero più piccolo. Riflettendo per qualche istante, si capisce facilmente che basta controllare se N sia divisibile per qualche numero inferiore o uguale a $\sqrt{N}$. Se N è abbastanza piccolo, diciamo di tre o quattro cifre, il calcolo può essere eseguito manualmente; con un normale computer da tavolo, si possono gestire numeri con più cifre. Ma l'impresa diviene irrealizzabile quando N ha, poniamo, cinquanta cifre o più. Esistono però altri modi per controllare se un numero N è primo, che non richiedono una ricerca a tutto campo dei possibili fattori fino a $\sqrt{N}$, e alcuni di essi sono abbastanza efficienti da funzionare bene anche per numeri con centinaia di cifre, se si utilizza un computer ragionevolmente veloce. Pertanto, trovare i numeri primi per generare le chiavi della crittografia a chiave pubblica non è un problema.

I metodi effettivamente utilizzati per verificare se un numero è primo vanno oltre lo scopo di questo libro, ma un semplice esempio dimostrerà come è possibile stabilire se un numero è primo senza dover guardare ed eliminare tutti i possibili fattori. L'esempio proviene dal lavoro del grande matematico francese Pierre de Fermat (1601-1665).

Sebbene si dedicasse alla matematica solo a livello «amatoriale» (di professione era un giurista), Fermat produsse alcuni dei risultati più intelligenti che la matematica abbia mai visto. Una delle sue osservazioni fu che se p è un numero primo, allora per ogni numero a inferiore a p , $a^{p-1} - 1$ è divisibile per p . Prendiamo, ad esempio, $p = 7$ e $a = 2$. Avremo:

$$a^{p-1} - 1 = 2^{7-1} - 1 = 2^6 - 1 = 64 - 1 = 63$$

e infatti 63 è divisibile per 7. Provate con qualunque valore di p (numero primo) e di a (inferiore a p) e vedrete che il risultato è sempre lo stesso.

Abbiamo così trovato un possibile modo per controllare se un numero n è primo oppure no. Calcoliamo il numero $2^{n-1} - 1$ e vediamo se è divisibile per n . Se non lo è, allora n non può essere primo (perché se fosse primo, in base alle osservazioni di Fermat $2^{n-1} - 1$ dovrebbe essere divisibile per n). Ma se scopriremo che $2^{n-1} - 1$ è divisibile per n , che cosa potremmo concludere? Purtroppo, non che n è necessariamente un numero primo (anche se è abbastanza probabile che lo sia). Il problema è che, sebbene il risultato di Fermat ci dica che $2^{n-1} - 1$ è divisibile per n ogniquale volta n è un numero primo, ciò non implica che non possano esistere numeri composti con la stessa proprietà (proprio come il fatto che tutte le automobili siano dotate di ruote non implica che non esistano altri oggetti con le ruote, come, ad esempio, le biciclette). E infatti esistono numeri non primi che godono della proprietà di Fermat. Il più piccolo è il numero 341, che non è primo, essendo il prodotto di 11 e 31. Se controllassimo (su un computer) scopriremmo che $2^{340} - 1$ è in effetti divisibile per 341 (come vedremo tra poco, non c'è bisogno di calcolare 2^{340} per effettuare questo controllo). I numeri composti che si comportano come numeri primi per quanto concerne la proprietà di Fermat sono chiamati pseudoprimi. Pertanto, se

usando la regola di Fermat scopriamo che $2^{n-1} - 1$ è divisibile per n , tutto quello che possiamo concludere è che n è un numero primo o pseudoprimo. (In questo caso ci sono probabilità molto più alte che n sia effettivamente un numero primo. Infatti, sebbene esistano infiniti numeri pseudoprimi, essi ricorrono molto meno frequentemente dei numeri primi. Ad esempio, esistono solo 2 numeri pseudoprimi sotto il 1000 e solo 245 sotto 1.000.000.)

Nell'effettuare il test descritto sopra, non occorre calcolare 2^{n-1} , un numero che sarebbe molto grande anche per valori piuttosto bassi di n . È sufficiente scoprire se $2^{n-1} - 1$ sia o meno divisibile per n . Ciò significa che, *a qualunque stadio del calcolo*, i multipli di n possono essere ignorati. In altre parole, ciò che occorre calcolare è il resto che *rimarrebbe* dividendo $2^{n-1} - 1$ per n . Lo scopo è vedere se questo resto è zero oppure no, ma poiché i multipli di n non influiscono sul resto, essi possono essere ignorati. I matematici (e i programmatori informatici) hanno un modo standard per denotare il resto di una divisione: il resto della divisione di A per B viene scritto con la notazione:

$$A \bmod B$$

Quindi, ad esempio, $5 \bmod 2$ è uguale a 1, $7 \bmod 4$ è uguale a 3 e $8 \bmod 4$ è uguale a 0.

Come esempio della prova di Fermat, applichiamo quanto detto al test per verificare se 61 sia o meno un numero primo. Dobbiamo calcolare il numero $[2^{60} - 1] \bmod 61$, che può anche essere scritto come $[2^{60} \bmod 61] - 1$. Se questo numero è diverso da zero, allora 61 non è un numero primo. Se è uguale a zero, allora 61 è un numero primo o è un numero pseudoprimo (e infatti, come già sappiamo, è un numero primo autentico). Proveremo a evitare di calcolare il grande numero 2^{60} . Iniziamo col notare che $2^6 = 64$ e che, pertanto, $2^6 \bmod 61 = 3$. Quindi, dato che $2^{30} = (2^6)^5$, otteniamo:

$$2^{30} \bmod 61 = (2^6)^5 \bmod 61 = (3)^5 \bmod 61 = 243 \bmod 61 = 60$$

Quindi,

$$2^{60} \bmod 61 = (2^{30})^2 \bmod 61 = 60^2 \bmod 61 = 3600 \bmod 61 = 1$$

Pertanto,

$$2^{60} \bmod 61 - 1 = 0$$

Dato che il risultato finale è 0, la conclusione è che 61 è un numero primo o è un numero pseudoprimo, come abbiamo anticipato.

Uno dei metodi che gli esperti utilizzano per trovare grandi numeri primi parte dal test di Fermat appena descritto e ne modifica l'approccio in modo da evitare di «farsi ingannare» da un numero pseudoprimo. La ragione per cui non possiamo descrivere questo metodo è che per superare il problema dei numeri pseudoprimi occorre un notevole lavoro e qualche sofisticato calcolo matematico.

Nonostante il grosso investimento di capacità e di lavoro, non è stato finora trovato alcun metodo per scomporre un grande numero in fattori primi che sia anche solo lontanamente paragonabile, in termini di efficienza, ai metodi per verificare se un

numero è primo. Tuttavia, anche in questo ambito, qualche successo c'è stato, e in svariate occasioni i matematici hanno proposto modi ingegnosi per trovare i fattori primi in un tempo computazionale ragionevolmente breve. Quando si cominciò a usare il sistema RSA, scomporre in fattori primi un numero di circa 120 cifre era il risultato massimo che si potesse ottenere. I progressi che furono compiuti successivamente sia nella creazione degli algoritmi sia nella tecnologia informatica resero vulnerabili questi numeri di 120 cifre, così che i crittografi dovettero aumentare le dimensioni delle chiavi ben oltre quel livello. Oggigiorno, molti matematici ritengono che una dimensione sicura per una chiave sia un numero di 300 cifre o più, essendo pressoché impossibile trovare un metodo capace (in tempi realistici) di scomporre in fattori primi un numero così grande.

Il fatto che i progressi nelle tecniche di scomposizione in fattori primi rappresentino una sfida autentica, seppur potenziale, per i codici RSA fu palesemente dimostrato nell'aprile del 1994, quando fu impiegato un metodo sofisticato per risolvere un problema nella crittografia RSA che era stato proposto nel 1977. L'origine del problema è di per sé interessante. Nel 1977, quando Rivest, Shamir e Adleman proposero il loro sistema di crittografia a chiave pubblica, esso fu descritto dallo scrittore Martin Gardner nel numero di agosto di *Scientific American*, all'interno della sua popolare rubrica di matematica. Lì Gardner presentava un breve messaggio che era stato codificato attraverso lo schema RSA, utilizzando una chiave di 129 cifre ottenuta dalla moltiplicazione di due grandi numeri primi. Il messaggio e la chiave erano stati prodotti da alcuni ricercatori del MIT, i quali offrivano, tramite Gardner, 100 dollari a chi per primo fosse riuscito a decifrare il codice. Il numero composto che costituiva la chiave per decifrare il codice divenne noto come RSA-129. A quel tempo si pensava che ci sarebbero voluti più di 20.000 anni per scomporre in fattori primi un numero di 129 cifre come quello, e pertanto il gruppo del MIT credeva che i suoi soldi fossero al sicuro. Ma due sviluppi successivi accelerarono i tempi e, soltanto diciassette anni dopo, il problema del MIT poté trovare una soluzione.

Il primo sviluppo fu la messa a punto dei cosiddetti metodi del crivello quadratico per scomporre grandi numeri in fattori primi. Una caratteristica cruciale di questi metodi, che si dimostrò importante per la fattorizzazione della chiave RSA-129, è che essi suddividevano efficacemente il problema in un gran numero di fattorizzazioni più piccole, un procedimento che, sebbene ancora assai difficile, per lo meno si poteva eseguire con un computer abbastanza veloce. Il secondo fondamentale sviluppo fu Internet. Nel 1993, Paul Leyland dell'Università di Oxford, Michael Graff della Iowa State University e Derek Atkins del MIT lanciarono un appello in Internet alla ricerca di volontari che fossero disposti a dedicare un po' di tempo per attuare, con l'ausilio dei loro computer, un massiccio assalto a RSA-129. L'idea era di distribuire le varie parti del problema di fattorizzazione ottenute con il metodo del crivello quadratico e poi attendere che fossero trovati abbastanza risultati parziali per produrre una fattorizzazione di RSA-129. (Il metodo del crivello quadratico che avevano utilizzato non richiedeva che tutte le sottofattorizzazioni venissero risolte, ma soltanto che ne fosse risolto un numero sufficiente.) Circa 600 volontari in tutto il mondo accolsero la sfida. Nel corso degli otto mesi successivi, i risultati arrivarono a

un ritmo di circa 30.000 al giorno. Nell'aprile del 1994, dopo aver raccolto più di otto milioni di singoli risultati, i tre scienziati affidarono a un potente supercomputer l'impresa formidabile di cercare una combinazione delle piccole fattorizzazioni che potesse portare a un fattore di RSA-129. Era un calcolo mastodontico, ma alla fine diede il risultato sperato. La chiave RSA-129 fu scomposta in due numeri primi, uno di 64 e l'altro di 65 cifre, e così l'originario messaggio del MIT poté essere decifrato. Esso recitava: *The magic words are squeamish ossifrage* (le parole magiche sono ossifrago schizzinoso). (Si tratta di un tipico scherzo tra i membri del MIT. L'ossifrago è un raro avvoltoio con un'apertura alare che può arrivare fino a tre metri, il cui nome significa «spaccaossa».)

Firme digitali

Un'altra questione di sicurezza che Whitfield e Hellman affrontarono nel loro articolo del 1976 era: come fa il ricevente di un documento elettronico a essere sicuro che esso sia stato effettivamente inviato dalla fonte da cui dichiara di provenire? Nel caso dei documenti scritti, ci si basa generalmente sulla firma. I sistemi di crittografia a chiave pubblica offrono un mezzo per creare un equivalente elettronico della firma: una firma digitale, per così dire. L'idea è semplice: si utilizza il sistema di crittografia a chiave pubblica al contrario. Se Alice vuole mandare a Carlo un documento con una firma elettronica, lo codifica utilizzando la sua chiave di decrittaggio segreta. Quando Carlo riceve il documento, utilizza la chiave pubblica di crittaggio di Alice per decifrare il messaggio. Questo risulterebbe incomprensibile a meno che non sia stato crittato utilizzando la chiave di decrittaggio di Alice. Dal momento che soltanto Alice conosce quella chiave, se il risultato è un documento leggibile, Carlo può essere sicuro che esso proviene da Alice.

In realtà, una firma digitale è una forma di autenticazione più sicura di una firma normale. Qualcuno potrebbe sempre copiare (a mano o per via elettronica) la vostra firma da un documento all'altro, mentre una firma digitale è legata al documento stesso. L'idea delle firme digitali è sfruttata anche per produrre certificati digitali, cioè attestati forniti da particolari siti web per dimostrare che sono davvero i siti che dicono di essere.

Che cosa tiene le password al sicuro?

Anche con la crittografia dei messaggi, alcune attività, come le operazioni bancarie online, hanno ancora dei punti deboli. Uno dei più ovvi è la password. Il fatto di trasmetterla in forma crittata garantisce che nessun intercettatore possa accedervi; ma se un hacker riuscisse a entrare nel computer in cui la vostra banca archivia le password dei suoi clienti (cosa che deve fare per poter controllare i tentativi di connessione dall'esterno), avrebbe immediatamente accesso libero al vostro conto corrente. Per evitare che ciò avvenga, le banche non archiviano le password nella loro

forma originaria, bensì in una versione «pasticciata» (*hashed*).

L'*hashing* è un processo particolare che prende una stringa di caratteri immessa da un utente (come la vostra password) e genera una nuova stringa di determinate dimensioni (strettamente parlando, non si tratta di un processo di criptaggio in quanto il mascheramento della password così ottenuto potrebbe essere irreversibile). Quando un cliente di una banca prova ad accedere al proprio conto corrente, il computer della banca confronta la versione camuffata della password introdotta con la stringa archiviata nel suo file di password mascherate. Affinché il sistema funzioni, la funzione di *hash*, H , deve godere di due proprietà piuttosto ovvie:

1. Per qualunque stringa di caratteri x , dovrebbe essere facile calcolare $H(x)$.
2. Dato un qualunque valore di *hash* y , dovrebbe essere computazionalmente impossibile trovare una stringa x tale che $H(x) = y$.

(«Computazionalmente impossibile» significa che il computer più veloce del mondo impiegherebbe più di, poniamo, una vita umana per portare a termine la procedura.)

Grazie al secondo requisito, anche se un hacker riuscisse ad accedere ai dati identificativi archiviati nel computer della vostra banca, non potrebbe comunque ottenere la vostra password (anche se, in assenza di controlli aggiuntivi, potrebbe sicuramente accedere al vostro conto corrente su quella macchina, dal momento che è la versione camuffata quella che il server ricevente utilizza per autorizzare la connessione).

Per ragioni pratiche, coloro che progettano le funzioni di *hash* solitamente richiedono un ulteriore requisito di uniformità che faciliti l'archiviazione delle versioni camuffate dei dati identificativi e renda possibile una procedura di ricerca nella banca dati più veloce e semplificata:

3. Tutti i valori prodotti da H devono avere la stessa lunghezza, cioè lo stesso numero di bit.

La conseguenza di questa terza condizione è che in teoria possono esserci molte stringhe di caratteri diverse che danno come risultato la medesima stringa camuffata; nel gergo tecnico, si dice che ci saranno inevitabilmente alcune «collisioni», cioè stringhe x e y differenti tali per cui $H(x) = H(y)$. Dato che l'accesso a siti sicuri è determinato (negli stessi siti) esaminando i dati camuffati introdotti per connettersi, un possibile punto debole del sistema è che, per accedere illegalmente a un conto corrente, l'intruso non deve necessariamente ottenere il codice identificativo e la password del titolare del conto; è sufficiente trovare *qualche* input che generi la medesima stringa camuffata; cioè, basta trovare un input che collida con i dati autentici. Nel progettare un algoritmo per una funzione di *hash*, è quindi importante assicurarsi che questa evenienza sia estremamente improbabile. Da ciò si ricava il quarto requisito:

4. Deve essere praticamente impossibile («computazionalmente impossibile») trovare una stringa y che collida con una data stringa x , cioè, tale per cui $H(x) = H(y)$.

Di solito, le funzioni di *hash* operano combinando (in qualche modo sistematico) i bit della stringa di input (ad esempio, i vostri dati identificativi) con altri bit scelti a caso, ed eseguendo qualche complicato processo iterativo di filtraggio che riduce la stringa risultante a una di una lunghezza determinata (prestabilita per il sistema). Attualmente sono in uso dozzine di funzioni di *hash* differenti. Le due più comunemente impiegate sono la MD5 (Message Digest Algorithm 5), messa a punto da Ronald Rivest (lo stesso del sistema RSA) al MIT nel 1991, tra tanti altri algoritmi di *hash* che aveva progettato, e la SHA-1 (Secure Hash Algorithm 1) creata dalla National Security Agency nel 1995. La MD5 produce una stringa cifrata a 128 bit, e richiederebbe in media 2^{64} tentativi per trovare una collisione. La SHA-1 genera una stringa di *hash* lunga 160 bit e, in questo caso, servirebbero in media 2^{80} tentativi per trovare una collisione. In teoria, entrambi i metodi sembrerebbero offrire un alto livello di sicurezza, ammesso che l'unico modo possibile per trovare una collisione sia per successive prove ed errori.

Sfortunatamente per il mondo della sicurezza digitale, il metodo per prove ed errori non è l'unico a minacciare un sistema di *hash* come SHA-1. Tra la fine degli anni '90 e l'inizio del 2000, Xiaoyun Wang, studiosa di matematica presso l'Università Tsinghua di Pechino, dimostrò che con un po' d'ingegno e di duro lavoro era possibile trovare collisioni per alcune funzioni di *hash* comunemente usate. Alla conferenza Crypto '04, tenutasi a Santa Barbara nel 2004, Wang sorprese i partecipanti annunciando un modo per trovare una collisione nella funzione MD5 in soltanto 2^{37} input, una straordinaria riduzione delle dimensioni del problema che rendeva il sistema altamente vulnerabile.

L'idea di Wang era di immettere nell'algoritmo stringhe che differiscono solo per pochi bit e guardare attentamente che cosa accade, passo per passo, man mano che l'algoritmo opera su di esse. Ciò la portò a sviluppare un «fiuto» per il tipo di stringhe che potevano portare a una collisione, il che le permise gradualmente di restringere il campo delle possibilità e di arrivare alla fine a mettere a punto una procedura per generare le collisioni.

Dopo l'annuncio alla Crypto '04, Wang e i suoi due colleghi Hongbo Yu e Yiqun Lisa Yin iniziarono a lavorare su quella che era considerata la più inespugnabile delle funzioni di *hash*: la SHA-1. Questa si rivelò un osso molto più duro della prima, ma, con sgomento (e ammirazione) di tutta la comunità dei ricercatori impegnati in questo campo, alla conferenza annuale sulla sicurezza informatica tenutasi a San Francisco nel febbraio del 2005 i tre studiosi annunciarono di aver creato un algoritmo potenzialmente in grado di generare una collisione per la funzione SHA-1 in soltanto 2^{69} passaggi.

Wang e i suoi colleghi non sono ancora riusciti a trovare una collisione per questo algoritmo; hanno solo prodotto un metodo che *potrebbe* trovarne una in molti meno passaggi di quanto si credesse possibile. 2^{69} è ancora un numero abbastanza grande da garantire al sistema un certo grado di sicurezza, almeno per ora. Lo stesso si può dire

dell'ancor migliore risultato di 2^{63} passaggi che Wang e altri collaboratori riuscirono a ottenere nei mesi che seguirono l'annuncio di febbraio 2005. Ma molti studiosi di crittografia informatica credono che il destino di questi sistemi sia ormai scritto e che, come conseguenza del lavoro di Wang, l'introduzione di metodi di calcolo sempre più veloci e potenti renderà presto inutili tutti gli algoritmi di *hash* attualmente in uso. Non accadrà oggi - gli esperti ci assicurano che le nostre operazioni bancarie agli sportelli automatici, per il momento, sono ancora sicure - ma presto. In un commento rilasciato alla rivista *New Scientist*, Burt Kaliski, direttore dei laboratori RSA di Bedford, nel Massachusetts, ha dichiarato: «Questo è un momento di crisi per la comunità di ricerca». Mark Zimmerman, un crittografo che lavora per i laboratori ICSA di Mechanicsburg, in Pennsylvania, parla in termini un po' più coloriti: «Non è Armageddon, ma è un bel calcio nel sedere».

QUANTO È AFFIDABILE LA PROVA?

*Dubbi sulle impronte digitali**L'uomo sbagliato?*

Quando Don arriva sulla scena del delitto scopre che l'assassino ha garrotato la vittima. Non è un metodo comune, ma ricorda a Don un omicidio commesso un anno prima. In quell'occasione, le indagini dell'FBI si erano concluse con successo. Dopo essere stato identificato da un testimone oculare e da un esame delle impronte digitali, l'assassino, un uomo di nome Carl Howard, aveva accettato di confessare, patteggiando la pena, ed era andato in prigione. Ma le somiglianze tra il precedente omicidio e quello nuovo sono così sorprendenti che Don inizia a domandarsi se, in quella precedente occasione, non avessero mandato in prigione l'uomo sbagliato. Mentre Charlie aiuta Don nelle indagini sul nuovo omicidio, i due discutono della possibilità che Howard fosse un uomo innocente condannato per un crimine che non aveva commesso.

Questa è la storia che gli spettatori hanno visto nell'episodio della prima serie di *NUMB3RS* intitolato *Crisi d'identità*, andato in onda in Italia il 17 giugno 2007.

La prova cruciale che aveva determinato la condanna di Howard era un'impronta digitale trovata sulla scena dell'omicidio, più precisamente l'impronta parziale di un pollice. L'esaminatrice dell'FBI era sicura della correttezza della sua identificazione, fatto che aveva indotto Howard e il suo avvocato a concludere che accettare il patteggiamento fosse l'unica opzione ragionevole. Ma, colto dal dubbio che Howard fosse innocente, Charlie, il matematico addestrato a pensare in maniera logica e a esigere sempre prove a supporto di una tesi scientifica, rivolge alcune domande all'esaminatrice:

CHARLIE: «Come fa a sapere che abbiamo tutti impronte digitali diverse?»

ESAMINATRICE «Semplice: perché non sono mai state trovate due persone con le stesse impronte digitali.»

CHARLIE: «Sono state esaminate le impronte digitali di tutte le persone che vivono su questo pianeta?»

La corrispondenza che l'esaminatrice aveva trovato si basava su quella che viene definita un'impronta parziale latente, ovvero sui segni lasciati solo da una porzione del polpastrello di un dito. Quindi Charlie continua il suo interrogatorio, domandando con quale frequenza accade che solo *una parte dell'impronta di un dito* di una persona assomigli a quella di un'altra persona. L'esaminatrice dice che non lo sa,

inducendo Charlie a incalzarla con altre domande:

CHARLIE: «Non ci sono dati disponibili?»

ESAMINATRICE: «No. Non abbiamo mai fatto un'indagine sull'intera popolazione.»

CHARLIE: «Ma la probabilità di avere una corrispondenza casuale non è l'unico modo per sapere realmente qual è la probabilità che due impronte combacino?»

AGENTE REEVES: «È così che funziona la prova del DNA.»

CHARLIE: «È per questo che diciamo che la prova del DNA ha una probabilità di errore di 'uno su un miliardo'. Ma per le impronte digitali non esistono probabilità di errore?»

Come sempre Charlie sta cogliendo nel segno. Oggigiorno le prove basate sulle impronte digitali, un tempo considerate così infallibili che nessuno avrebbe mai osato metterne in dubbio l'attendibilità, stanno subendo continui attacchi e critiche nei tribunali degli Stati Uniti e di molti altri Paesi.

Il mito delle impronte digitali

Una delle conquiste più sorprendenti del XX secolo in ambito legale consiste probabilmente nell'aver elevato l'identificazione delle impronte digitali a «sistema aureo» per l'evidenza scientifica nei procedimenti giudiziari. La sua accettazione come «prova decisiva» pressoché inattaccabile nelle aule di tribunale è dimostrata dalla terminologia che viene spesso applicata per indicare il suo unico rivale attuale, la prova del DNA che, per l'appunto, viene spesso chiamata «impronta digitale genetica».

Quando apparve originariamente, il metodo delle impronte digitali non fu subito accolto come la chiave magica per risolvere i problemi di identificazione dei criminali. Sia negli Stati Uniti sia in Europa, la nuova tecnica impiegò decenni per scalzare il suo predecessore, il sistema Bertillon.

Inventato da un funzionario della polizia di Parigi nel tardo XIX secolo, il sistema Bertillon si basava principalmente su un complicato insieme di undici misure anatomiche accuratamente registrate: la lunghezza e la larghezza della testa, la lunghezza del dito medio della mano sinistra, la distanza tra il gomito sinistro e la punta del dito medio della mano sinistra e così via. Il sistema si era rivelato molto efficace soprattutto con i trasgressori recidivi che tentavano di evitare sentenze più severe ricorrendo a una serie di falsi nomi.

Come il sistema Bertillon, l'identificazione delle impronte digitali si dimostrò un metodo di «accertamento» affidabile. Con questa tecnica, un dipartimento di polizia poteva confrontare un insieme di dieci impronte digitali ad alta qualità ottenute da un certo «Mario Rossi», arrestato per qualche crimine, con un archivio di «serie complete» di dieci impronte digitali prese da precedenti colpevoli, e magari scoprire

che Mario Rossi era in realtà «Luigi Bianchi», un delinquente uscito dal carcere poco tempo prima. Ancor più sorprendente era la possibilità di «prelevare» le impronte digitali da una superficie - un tavolo, una finestra, un bicchiere - nel luogo di un crimine e di usare queste «impronte latenti» per identificare il colpevole. Vale a dire, gli investigatori potevano compiere una ricerca in uno schedario contenente esemplari noti, cioè serie complete di impronte digitali di individui conosciuti, per verificare se ce ne fosse uno che corrispondeva alle impronte ritrovate sulla scena del delitto e identificare in tal modo il colpevole. Oppure potevano prendere le impronte digitali di un sospetto e confrontarle con quelle prelevate dalla scena del delitto. Sebbene le impronte digitali latenti siano spesso di bassa qualità - sbavate, parziali (riguardanti solo una porzione del polpastrello del dito), incomplete (riguardanti, poniamo, solo un dito o due) - un esaminatore abile ed esperto potrebbe tuttavia essere in grado di osservare un numero di somiglianze con un esemplare noto tale da consentirgli di identificare il colpevole con un grado di sicurezza sufficiente per deporre in tribunale.

Dato che la probabilità che un'indagine condotta sulla scena del delitto porti a misure precise di caratteristiche biometriche del colpevole come la larghezza della testa è pressoché nulla, il vantaggio del metodo delle impronte digitali rispetto al sistema Bertillon per il lavoro investigativo divenne presto evidente. Ma anche nel momento in cui lasciava il posto alla nuova tecnica di identificazione, il sistema Bertillon manteneva ancora un chiaro vantaggio: il sistema di indicizzazione a esso associato. Questo sistema, infatti, si basava su valori numerici annessi a misure biometriche standard; di conseguenza, la ricerca in un grande schedario per trovare una possibile corrispondenza con le misure di una persona sotto custodia poteva essere condotta in modo semplice e obiettivo. Il metodo delle impronte digitali, invece, si basava sul giudizio umano nel confronto fianco a fianco delle caratteristiche distintive di due impronte o insiemi di impronte, e non era pertanto soggetto allo stesso tipo di efficienza numerica.

Tuttavia a metà del XX secolo, con l'avvento dei computer, divenne possibile codificare numericamente le serie di impronte digitali in un modo che consentiva di eliminare rapidamente la grande maggioranza delle potenziali corrispondenze e limitare la ricerca a un piccolo sottoinsieme del grande archivio iniziale. L'esaminatore umano poteva intervenire solo a quel punto, per effettuare l'identificazione finale: una possibile corrispondenza tra l'impronta di un sospetto e un singolo esemplare. In realtà, dopo l'11 settembre 2001, il governo degli Stati Uniti intensificò l'impegno nello sviluppo di metodi per confrontare rapidamente, con l'ausilio di computer, le scansioni delle impronte digitali di individui che cercavano di entrare nel Paese con quelle archiviate in banche dati di terroristi noti o sospetti. Questi metodi assistiti da strumentazioni informatiche, noti agli esperti di impronte digitali come sistemi *semi-lights-out*, sono quasi interamente basati su sintesi delle caratteristiche chiave delle impronte digitali degli individui codificate in termini numerici. Sfruttando queste caratteristiche è possibile offrire a un esperto umano, il cui giudizio finale è considerato irrinunciabile, non più di una manciata di esemplari da controllare per individuare un'eventuale corrispondenza.

Nei procedimenti giudiziari, quello dell'esperienza umana si è dimostrato un fattore cruciale. Gli esaminatori di impronte digitali, che lavorano per l'FBI o altre

forze di polizia, hanno vari livelli di esperienza e competenza, ma le loro deposizioni in tribunale poggiano sempre su due pilastri fondamentali:

- la tesi che le impronte digitali sono uniche e caratteristiche di ogni singolo individuo: non sono mai state trovate due persone, nemmeno due gemelli identici, con le stesse impronte digitali;
- la sicurezza dell'esaminatore che dice di essere convinto «al cento per cento» (o qualcosa di altrettanto persuasivo) che le impronte ritrovate sulla scena del delitto e quelle dell'imputato corrispondono esattamente e devono quindi essere impronte della stessa persona.

Come vengono «confrontate» le impronte digitali?

Non esiste un protocollo definito per confrontare le impronte digitali, ma gli esperti generalmente rappresentano le immagini delle impronte più o meno in questo modo:



Impronta trovata sulla scena del delitto Singolo dito da un esemplare

Per effettuare un'identificazione, un esaminatore abile ed esperto esegue molteplici confronti. Nel farlo, si affida a un principio ammirevolmente logico, il principio dell'unica dissomiglianza, il quale afferma che se tra due impronte si osserva anche soltanto una differenza che non può essere spiegata in nessun modo - cioè che non può essere interpretata, poniamo, come il risultato di una sbavatura o di una macchiolina - si deve escludere la possibilità di una corrispondenza tra le due impronte esaminate.

La testimonianza più comune poggia, tuttavia, sulla determinazione di talune caratteristiche chiamate *minutiae*, cioè i punti in cui le creste delle impronte digitali terminano o si biforcano. Queste sono talvolta chiamate punti di Galton, in omaggio all'inglese Sir Francis Galton, un pioniere della statistica che in un libro del 1892, intitolato *Finger Prints*, aveva stabilito i metodi fondamentali per confrontare questi punti in due impronte al fine di compiere un'identificazione. Sfortunatamente per la pratica che sfrutta il confronto delle impronte digitali in ambito legale, non è stato stabilito alcun criterio universalmente valido per definire il numero minimo di punti in comune necessari per compiere un'identificazione attendibile. Più di un avvocato difensore e più di un giudice si è trovato in difficoltà per questa mancanza di un criterio comune che definisca il numero di punti da considerare: ne bastano dodici? Oppure otto? In Australia e in Francia il numero minimo è dodici. In Italia è sedici. Negli Stati Uniti non è stata data un'impronta comune (non è un gioco di parole), ma le regole variano da uno Stato all'altro, persino da un distretto di polizia all'altro. In sostanza, la posizione degli esperti di impronte digitali in tribunale è sempre qualcosa

del genere: «Solitamente richiedo almeno X punti», dove X non è mai più grande del numero di punti che l'esperto ha considerato in quella particolare occasione.

Gli esperti di impronte digitali si scontrano con i matematici come Charlie Eppes

Negli ultimi anni l'accettazione automatica nei tribunali della presunta certezza delle identificazioni compiute dagli esperti di impronte digitali è stata contrastata da un crescente coro di opposizione. Come Charlie Eppes, diversi matematici, statistici e altri scienziati, così come illustri avvocati e persino alcuni giudici, hanno espresso lamentele in tribunale e in pubblico circa la mancanza di criteri standard per valutare le prove fornite dagli esaminatori di impronte digitali, riguardo alla certificazione delle prestazioni degli stessi esaminatori e, cosa più importante di tutte, circa la mancanza di verifiche scientificamente controllate delle identificazioni effettuate mediante il confronto delle impronte digitali, cioè la mancanza di una base per determinare la frequenza di errori.

Facendo riferimento a un acronimo usato per indicare i comuni metodi di identificazione delle impronte digitali, ACE-V, un giudice federale americano ha commentato:¹⁶

La corte trova anche che, per quanto la metodologia ACE-V sembri suscettibile di controllo, tale controllo non è ancora stato effettuato.

Per un esperto nel metodo di indagine scientifica, è semplicemente sbalorditivo sentir giustificare le identificazioni delle impronte digitali con la frase «non ne esistono due uguali». Questa è, al massimo, la risposta giusta alla domanda sbagliata. Anche se tutti i mille miliardi e più di possibili coppie ricavabili dai 150 milioni di «esemplari» completi di impronte raccolti nella banca dati civile dell'FBI fossero accuratamente esaminati dal migliore esperto umano e si dimostrassero in accordo con il principio «non ne esistono due uguali», il livello di garanzia fornito dall'affermazione di per sé sarebbe minimo. La domanda giusta da porsi è: con che frequenza gli esperti si sbagliano quando dichiarano di aver trovato una corrispondenza tra un esemplare ad alta qualità composto dalle impronte di dieci dita e le impronte parziali imperfette di due dita ritrovate sulla scena di un reato?

C'è un'evidente ironia nel fatto che la prova del DNA (discussa nel capitolo 7), la quale negli anni '80 e '90 riuscì solo gradualmente, e solo per mezzo di accurati controlli scientifici, a ottenere credibilità nelle aule di tribunale come «impronta digitale genetica», venga oggi citata come lo standard per convalidare la presunta attendibilità delle identificazioni delle impronte digitali. L'attenta fondazione scientifica che fu edificata allora, producendo dati e utilizzando la teoria delle probabilità e l'analisi statistica per rispondere a domande sulla probabilità di corrispondenze errate tra i campioni di DNA, finora è riuscita a stabilire un «unico

¹⁶ *United States v. Sullivan*, 246 E Supp. 2d 700, 704 (E.D. Ky. 2003).

punto di paragone» - per quanto assai incisivo - con l'identificazione delle impronte digitali. La domanda di Charlie, «Non esistono probabilità di errore anche per le impronte digitali?», non si sente solo in televisione.

Nel 2005, appena dopo Natale, la corte suprema del Massachusetts decretò che, nel nuovo processo contro Terry L. Patterson, gli avvocati dell'accusa non potevano presentare in tribunale la testimonianza di un perito che aveva trovato una corrispondenza tra le impronte digitali dell'imputato e quelle ritrovate nell'automobile di un investigatore della polizia di Boston assassinato nel 1993. La decisione fu presa dopo che la corte aveva chiesto la consulenza legale di una varietà di scienziati e di esperti legali (in qualità di *amici curiae*, cioè «amici della corte») circa l'affidabilità delle identificazioni basate sulle «impronte simultanee». Nello specifico, l'esaminatore del distretto di polizia di Boston era pronto a testimoniare che tre impronte parziali ritrovate nell'automobile dell'investigatore, in base ad alcuni indizi decisivi, sembravano essere state prodotte nello stesso momento, e quindi dallo stesso individuo, e che, secondo la sua analisi, rivelavano diversi punti in comune con le impronte dell'imputato e più precisamente: sei in un dito, due in un secondo dito e cinque in un terzo.

Anche per gli approssimativi standard degli esperti di impronte digitali americani riguardo al numero minimo di punti in comune richiesti per dichiarare una corrispondenza, questa combinazione di diverse dita con soltanto pochi punti in comune per ognuna - cioè, l'uso delle «impronte simultanee» - è un po' forzato. Benché almeno uno dei documenti presentati dagli *amici curiae*, firmato da una squadra di eminenti statistici, scienziati e studiosi di legge, avesse chiesto alla corte di decretare che *tutte le identificazioni di impronte digitali venissero escluse* dai processi finché non ne fosse stata provata la validità e non ne fosse stata stabilita la frequenza di errore, la corte (forse abbastanza prevedibilmente) limitò la decisione a quel caso particolare.

Gli argomenti avanzati nel caso Patterson e in molti altri casi simili citavano esempi recenti di errori nelle identificazioni delle impronte digitali presentate nel corso di processi penali. Uno di questi era il caso di Stephan Cowans, il quale nel 1997 era stato dichiarato colpevole dell'omicidio di un poliziotto di Boston sulla base di una testimonianza oculare e dell'identificazione dell'impronta di un pollice ritrovata su un bicchiere che l'assassino aveva usato per bere dell'acqua. Dopo aver scontato sei dei trentacinque anni di carcere cui era stato condannato, Cowans era riuscito a guadagnare abbastanza denaro in prigione per pagare un test del DNA sul materiale usato come prova. Il test lo scagionò e l'uomo fu alla fine rilasciato.

Nel 1999, in un altro caso famoso, gli avvocati che difendevano Byron Mitchell da un'accusa di rapina a mano armata misero in dubbio l'attendibilità della sua identificazione sulla base di due impronte prelevate dall'automobile che il rapinatore aveva usato per scappare. Per dare sostegno agli argomenti dell'accusa sull'ammissibilità della testimonianza del loro esperto di impronte digitali, l'FBI mandò le due impronte e l'esemplare completo di Mitchell a cinquantatré laboratori legali. Questo test non fu altrettanto rigoroso di quelli proposti dagli scienziati, basati sul confronto tra gruppi campione di impronte digitali. Nondimeno, dei trentanove laboratori che mandarono indietro il proprio parere, nove (il 23 per cento)

dichiararono che le impronte di Mitchell *non* corrispondevano a quelle ritrovate nell'automobile. Il giudice, tuttavia, respinse le obiezioni della difesa e Mitchell fu dichiarato colpevole e mandato in prigione. Da allora l'FBI non ha più ripetuto questo genere di controllo e continua a sostenere che non è mai successo che uno dei loro esperti di impronte digitali abbia deposto in tribunale basandosi su una corrispondenza errata. Tale affermazione, però, rimane appesa a un filo sottile, soprattutto alla luce della storia che segue.

Il caso Brandon Mayfield: un fiasco dell'FBI

La mattina dell' 11 marzo 2004, in una serie coordinata di attentati sui treni dei pendolari di Madrid, 191 persone persero la vita e più di duemila rimasero ferite. La colpa fu attribuita agli estremisti islamici locali ispirati da al-Qaeda. Gli attentati avvennero tre giorni prima delle elezioni spagnole, in occasione delle quali gli elettori, adirati, cacciarono il governo conservatore che aveva appoggiato le manovre americane in Iraq. Le ripercussioni in Europa e in tutto il mondo furono enormi. Non sorprende, quindi, che l'FBI fosse ansiosa di offrire il proprio aiuto quando ricevette dalle autorità spagnole una copia digitale delle impronte che erano state trovate su un sacchetto di plastica pieno di detonatori vicino a uno dei luoghi degli attentati, impronte che gli investigatori spagnoli non erano stati in grado di identificare. La banca dati dell'FBI conteneva anche le impronte di un avvocato di Portland di trentasette anni, di nome Brandon Mayfield, archiviate quando questi aveva prestato servizio come luogotenente nell'esercito degli Stati Uniti. Nonostante la qualità relativamente bassa delle immagini digitali inviate dagli investigatori spagnoli, tre esaminatori della Latent Fingerprint Unit dell'FBI sostennero di aver trovato una corrispondenza tra le impronte ritrovate sul luogo del reato e quelle di Mayfield. Per quanto Mayfield non fosse mai stato in Spagna, l'FBI era comprensibilmente interessata a trovare una corrispondenza con le sue impronte digitali: negli anni '80 l'uomo si era convertito alla religione islamica e aveva già attirato l'attenzione difendendo un sospetto terrorista musulmano, Jeffrey Battle, in un caso di custodia minorile. Agendo in base al Patriot Act americano, l'FBI per due volte entrò di nascosto nella sua casa e portò via potenziali prove, tra cui computer, carte, copie del Corano, e quelli che furono chiamati «documenti spagnoli», ma che in realtà, come si scoprì in seguito, erano semplicemente i compiti a casa di uno dei figli di Mayfield. Sicura di aver scovato qualcuno che non solo aveva impronte digitali corrispondenti a quelle ritrovate nel luogo di uno degli attentati ma che era anche plausibilmente coinvolto nel complotto di Madrid, l'FBI arrestò Mayfield, il quale fu tenuto sotto custodia come «testimone materiale».

Dopo due settimane l'uomo fu rilasciato, ma i sospetti sulla sua colpevolezza e le restrizioni sui suoi spostamenti furono revocati solo quattro giorni dopo, quando un giudice federale fermò l'azione giudiziaria contro di lui, sostanzialmente perché le autorità spagnole, nel frattempo, avevano ricollegato le originarie impronte digitali latenti a un algerino. Si scoprì che *prima* di incarcerare Mayfield l'FBI era a

conoscenza del fatto che la polizia scientifica spagnola non condivideva il parere degli esperti dell'FBI in merito alla corrispondenza tra le sue impronte digitali e quelle ritrovate sulla scena del crimine. Dopo la deliberazione del giudice, che ordinò la restituzione di tutti gli oggetti e i documenti personali presi dalla casa di Mayfield, l'FBI si scusò con lui e con la sua famiglia per «i problemi arrecati da questa faccenda».

Il procuratore dell'Oregon Karin Immergut dovette darsi molto da fare per dimostrare che Mayfield non era stato preso di mira a causa della sua religione o dei clienti che aveva rappresentato. In realtà, i verbali del tribunale suggerivano che l'errore iniziale fosse dovuto a un supercomputer che aveva selezionato le impronte di Mayfield dalla sua banca dati, e che quell'errore fosse stato poi aggravato dagli analisti dell'FBI. Come prevedibile, il governo condusse diverse indagini su questo imbarazzante insuccesso del sistema dell'FBI per l'identificazione delle impronte digitali, che gode di grande reputazione. In base a quanto fu riferito in un articolo apparso sul *New York Times* il 17 novembre 2004, una squadra internazionale di esperti capitanata da Robert B. Stacey, direttore della Quality-Assurance Unit del laboratorio dell'FBI di Quantico, in Virginia, concluse che i due periti cui era stato chiesto di confermare il parere del primo esperto avevano ripetuto l'errore perché «il costume dell'FBI dissuade gli esaminatori di impronte digitali dall'essere in disaccordo con i loro superiori». Tanto basti per sfatare il mito dello scienziato imparziale e obiettivo.

Che cosa dovrebbe fare un povero matematico?

Nel regno della televisione, Don e Charlie non si daranno pace finché non scopriranno non solo chi è stato a garrotare la vittima nel nuovo caso di omicidio, ma anche se Carl Howard era innocente del precedente delitto e, in questo caso, chi era il vero colpevole. Come prevedibile, entro i quarantadue minuti dell'episodio (il tempo totale ripartito tra gli annunci pubblicitari), Charlie riesce ad aiutare Don e i suoi colleghi a smascherare il vero colpevole - *di entrambi i crimini* - che si scopre essere lo stesso testimone oculare che aveva identificato Howard (un conflitto di interessi che non si verifica molto spesso nei casi veri). L'identificazione di Carl Howard sulla base del confronto delle impronte digitali era stato un errore bello e buono.

Dato l'assai poco rassicurante stato delle cose nel mondo reale, dove incombe sempre minacciosamente la possibilità che le identificazioni delle impronte digitali siano messe in dubbio, sia nei nuovi casi di crimine sia negli appelli per la riapertura di vecchi casi, molti matematici e statistici, insieme ad altri scienziati, vorrebbero fare qualcosa. Nessuno dubita seriamente che le impronte digitali costituiscano uno strumento molto prezioso per gli investigatori e per gli avvocati dell'accusa. Ma i principi di imparzialità e integrità che sono parte dei fondamenti stessi del sistema giudiziario e di quel sistema di saperi che chiamiamo scienza richiedono che lo studio e l'analisi dell'attendibilità delle prove basate sulle impronte digitali vengano intrapresi senza ulteriori insensati ritardi. La frequenza di errori nella determinazione

delle corrispondenze tra impronte digitali dipende chiaramente da diversi fattori matematicamente quantificabili, quali:

- le capacità dell'esperto;
- il protocollo e il metodo seguiti dall'esperto nel processo di individuazione;
- la qualità dell'immagine, la sua completezza e il numero di dita nei campioni da confrontare;
- il numero di possibili corrispondenze che si chiede all'esperto di considerare per l'impronta di un sospetto;
- il tempo disponibile per compiere l'analisi;
- le dimensioni e la composizione dell'insieme di esemplari disponibile per il confronto;
- la frequenza con cui si osservano forti somiglianze tra impronte parziali o complete di singole dita di persone diverse.

Forse ciò che maggiormente stimolerà la considerazione di tali fattori quantificabili nei prossimi anni non saranno le esigenze del sistema giudiziario penale, bensì il bisogno di uno sviluppo e di un miglioramento sostanziale nell'ambito, ad esempio, dei «sistemi biometrici di sicurezza» e dei sistemi automatizzati di rapida analisi delle impronte digitali al servizio della sicurezza interna.

Impronte digitali in rete

Mentre il XX secolo volgeva al termine, la collezione di impronte digitali dell'FBI, iniziata nel 1924, era arrivata a contenere più di duecento milioni di schede indicizzate, archiviate in oltre duemila schedari, una fila dietro l'altra, che occupavano approssimativamente cinquemila metri quadri di spazio nella sede della Criminal Justice Information Services Division dell'FBI a Clarksburg, nella Virginia occidentale. L'FBI riceveva ogni giorno più di 30.000 richieste di confronto di impronte digitali. Era chiaro che bisognava ricorrere alla memorizzazione elettronica e alla ricerca automatica.

La sfida era trovare il modo più efficiente per codificare versioni digitalizzate delle immagini delle impronte. (La pratica di catturare subito le immagini in forma digitale fu introdotta più tardi, incrementando il grado di efficienza, ma aumentando allo stesso tempo le preoccupazioni legali circa l'attendibilità di queste prove cruciali, considerata la facilità con cui le immagini digitali possono essere alterate.) La soluzione scelta faceva uso di una branca relativamente nuova della matematica chiamata «teoria delle ondine» (*Wavelet theory*). La scelta portò alla determinazione di uno standard nazionale: l'algoritmo della trasformata *Wavelet* discreta, noto anche come algoritmo WSQ (*Wavelet/Scalar Quantization*).

Come l'assai più famoso standard di codifica delle immagini digitali JPEG-2000, anch'esso basato sulla teoria delle ondine, WSQ è sostanzialmente un algoritmo di compressione che processa l'immagine digitale originale per produrre un file che

occupa meno memoria. Se scansiono con una risoluzione di 500 pixel per pollice, un esemplare completo di impronte digitali genererà un file di circa 10 MB. Negli anni '90, quando il sistema fu introdotto per la prima volta, questo significava non solo la necessità di un grande spazio di memoria per l'archiviazione dei file, ma anche, e soprattutto, notevoli difficoltà nel trasferire rapidamente i file da una parte all'altra del Paese (e nel resto del mondo), magari ad agenti in località remote, servite solo da lente connessioni via modem. Il sistema WSQ riduce le dimensioni dei file di venti volte, il che significa che il file risultante peserà soltanto 500 KB. Ecco un altro esempio del potere della matematica. A essere precisi, nel processo qualche dettaglio va perduto, ma si tratta sempre di dettagli impercettibili all'occhio umano, anche quando l'immagine risultante viene ingrandita diverse volte per operare un confronto visivo.¹⁷

L'idea che sta dietro alla codifica (e alla compressione) *Wavelet* risale al lavoro compiuto all'inizio del XIX secolo dal matematico francese Joseph Fourier, il quale aveva dimostrato che qualunque funzione usata per esprimere fenomeni del mondo reale, che parta da numeri reali e produca numeri reali, può essere rappresentata come una somma di multipli delle familiari funzioni seno e coseno (figura 7). Fourier era interessato alle funzioni che descrivono la dissipazione del calore, ma i suoi risultati valgono per una grande quantità di funzioni, comprese quelle che descrivono le immagini digitali. (Da un punto di vista matematico, un'immagine digitale è una funzione, nello specifico una funzione che assegna a ogni pixel un numero indicante un particolare colore o una determinata sfumatura di grigio.) Quasi sempre, per riprodurre una funzione che descrive un fenomeno del mondo reale occorre sommare tra loro infinite funzioni seno e coseno, ma Fourier fornì un metodo per farlo, in particolare per calcolare il coefficiente di ogni funzione seno e coseno della somma.

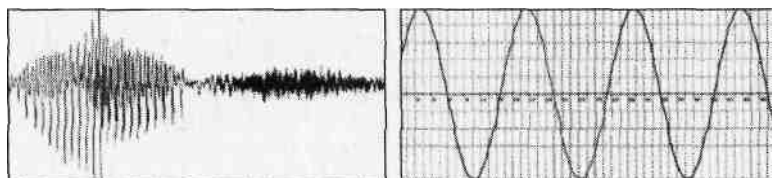


Figura 7. Nell'analisi di Fourier, un'onda (come l'onda sonora mostrata nella figura a sinistra) è rappresentata come una somma infinita di onde sinusoidali di diversa frequenza e ampiezza (figura a destra).

La complessità dell'analisi di Fourier, e la ragione per cui essa generalmente richiede un numero infinito di addendi seno e coseno per generare una data funzione, risiede in parte nel fatto che le funzioni seno e coseno vanno avanti all'infinito, seguendo un regolare andamento ondulatorio. Negli anni '80, alcuni matematici provarono per gioco a compiere l'analisi di Fourier utilizzando porzioni finite di un'onda, le cosiddette ondine (figura 8). La funzione che genera un'ondina è più complicata delle funzioni seno e coseno, ma la maggiore complessità della funzione è

¹⁷ Inizialmente l'FBI aveva considerato l'ipotesi di utilizzare lo standard JPEG, ma considerando la particolare natura delle immagini delle impronte digitali - sostanzialmente composte da linee curve «nere» parallele separate da stretti spazi su uno sfondo «bianco» - concluse che un sistema progettato su misura sarebbe stato molto più efficiente. In molti casi, ad esempio in presenza di sfondi abbastanza uniformi, JPEG-2000 può arrivare a comprimere le dimensioni dell'immagine fino a duecento volte.

più che compensata dalla notevole semplificazione della rappresentazione risultante. L'idea è di iniziare con una singola «ondina madre» e poi creare le figlie traslando (spostando) la madre di un'unità o altrimenti espandendola o contraendola alternativamente di una potenza di 2. La funzione sarà poi espressa come una somma di ondine figlie generate da un'unica madre.

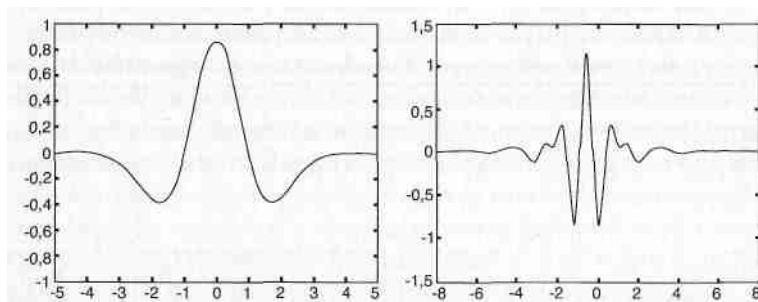


Figura 8. Ondine. Quella a sinistra è chiamata, per ovvie ragioni, il «sombbrero».

La teoria delle ondine vide il suo vero decollo nel 1987, quando Ingrid Daubechies, dei laboratori AT&T Bell, costruì una famiglia di ondine che rendeva questo processo particolarmente efficiente quando i calcoli venivano eseguiti su un computer. Non molto tempo dopo l'FBI iniziò a considerare seriamente l'ipotesi di utilizzare le ondine per codificare le impronte digitali. Anziché codificare i bit che costituiscono l'immagine digitalizzata di un'impronta, il computer dell'FBI codifica i parametri numerici (coefficienti) chiave nella rappresentazione *Wavelet* della funzione dell'immagine. Quando un agente di polizia vuole che una determinata serie di impronte digitali venga mostrata sullo schermo di un computer oppure stampata, il computer in realtà *ricrea* l'immagine utilizzando i coefficienti memorizzati nel file.

Una volta che le impronte digitali sono state codificate come sequenze di numeri, diviene relativamente semplice compiere ricerche automatiche su un computer al fine di individuare una corrispondenza tra una delle impronte contenute nella banca dati e una trovata, poniamo, sulla scena di un delitto. Il computer andrà a cercare le stringhe di numeri che risultano molto simili a quella proveniente dal campione. (Occorre adottare un approccio matematico sofisticato per decidere che cosa voglia dire «molto simili» in una situazione del genere; al di là di questo, il processo è semplice.)

Un aspetto affascinante della codifica *Wavelet* è che essa coglie automaticamente le stesse caratteristiche di un'immagine che colgono i nostri occhi. I coefficienti nella rappresentazione finale corrispondono a pixel molto diversi dai pixel vicini, e posti solitamente sui contorni degli oggetti contenuti nell'immagine. Ciò significa che le ondine ricreano un'immagine principalmente disegnandone i contorni, che è proprio quello che facciamo anche noi quando abbozziamo un disegno. Alcuni ricercatori hanno suggerito che l'analogia tra le trasformate *Wavelet* e la vista umana non è accidentale, e che i nostri neuroni filtrano i segnali visivi in modo simile alle ondine.

CONNETTERE I PUNTI

*La matematica delle reti**Una questione in sospeso*

Una bomba artigianale esplode sotto un'automobile parcheggiata fuori da un ufficio di reclutamento dell'esercito degli Stati Uniti nel centro di Los Angeles, uccidendo un pedone che camminava nelle vicinanze e ferendo sua moglie. L'episodio ricorda in tutto e per tutto un altro attentato compiuto esattamente trentacinque anni prima come gesto di protesta contro la guerra nel Vietnam. Uguale è anche il messaggio inviato all'FBI (questa volta via mail), contenente una dichiarazione di responsabilità e la promessa di ulteriori attacchi, con l'unica differenza che questa volta la parola «Vietnam» è stata sostituita con «Iraq».

L'FBI aveva sempre creduto che l'attentato del 1971 fosse opera di un dimostrante pacifista di nome Matt Stirling che era scappato subito dopo e non era mai stato catturato. Il primo pensiero di Don è che Stirling sia ritornato per eseguire una sorta di replica commemorativa del passato gesto di protesta, e quindi recupera tutti i documenti relativi al caso precedente.

Tuttavia, non è ancora escluso che si tratti di una semplice imitazione compiuta da qualche altra persona o gruppo. Ma se così fosse, i nuovi responsabili dovrebbero aver avuto accesso ad alcune informazioni dettagliate sull'episodio precedente, e quindi il vecchio caso potrebbe comunque fornire qualche indizio su chi ha organizzato il nuovo attentato. Comunque siano andate le cose, Don deve raccogliere tutte le informazioni che può sull'attentato del 1971. Charlie osserva suo fratello alle prese con questa montagna di dati.

DON: «Al momento Stirling è il sospetto numero uno. Ma trentacinque anni sono tanti per trovare una pista da seguire».

CHARLIE: «Ma sembra che tu abbia molti dati sul caso originale. Potrei usare una branca della matematica chiamata analisi delle reti sociali; è un metodo che analizza la struttura dei gruppi, come si sviluppano le linee di connessione, per rivelare schemi nascosti. Ci può aiutare a scoprire il ruolo di Stirling nell'organizzazione, il che a sua volta ci può dire con chi lavorava e su chi aveva influenza».

DON: «La tua matematica potrebbe dirci se si tratta di un'imitazione?»

CHARLIE: «Identificherò i sospetti più probabili, e scoprirò se Stirling fa parte o meno della lista».

E così che agli spettatori dell'episodio della seconda serie di *NUMB3RS*, *Una questione in sospeso*, in onda in Italia il 26 agosto 2007, è stata presentata l'analisi delle reti sociali, una branca relativamente nuova della matematica divenuta estremamente importante sulla scia degli eventi dell'11 settembre 2001.

Un nuovo tipo di guerra, un nuovo tipo di matematica

Gli eventi dell'11 settembre 2001 cambiarono istantaneamente il modo degli americani di percepire le parole «terrorista» e «rete», e gli Stati Uniti, così come altri Paesi, iniziarono presto a prepararsi a combattere un nuovo tipo di guerra contro un nuovo genere di nemico. Nelle tradizionali operazioni militari, condotte in luoghi specifici, era importante conoscere il territorio in cui le battaglie sarebbero state combattute. Nella guerra contro il terrorismo, non esiste un luogo specifico. Come gli attentati dell'11 settembre hanno dimostrato fin troppo bene, il campo di battaglia può essere ovunque. La base del potere dei terroristi non è geografica; piuttosto, essi operano attraverso reti, con membri distribuiti in tutto il globo terrestre. Per combattere un simile nemico, occorre conoscere il nuovo «territorio»: le reti, il modo in cui sono costruite e come operano.

Lo studio matematico delle reti, noto come teoria o analisi delle reti, si basa su una branca della matematica pura chiamata teoria dei grafi, che studia le connessioni tra i punti di un insieme. Facendo uso delle tecniche della teoria dei grafi e dell'analisi delle reti per studiare le reti sociali, come quelle terroristiche, i matematici hanno creato una sottodisciplina specializzata chiamata analisi delle reti sociali o SNA (*Social Network Analysis*). La SNA ha visto un rapido sviluppo negli anni immediatamente precedenti l'11 settembre 2001 ed è diventata da quel momento in poi una materia ancor più scottante. L'applicabilità della SNA per combattere il crimine e il terrorismo era nota agli specialisti da molti anni, ma fu solo dopo che venne alla luce il complotto di al-Qaeda dell'11 settembre che la gente comune si rese conto dell'importanza cruciale della «connessione dei punti» nelle indagini e nella sorveglianza contro il terrorismo.

Gli attacchi dell'11 settembre come caso di studio

I fatti fondamentali sono oggi ben noti: la mattina dell'11 settembre 2001 quattro aerei di linea furono dirottati e trasformati in armi d'attacco da parte dei terroristi di al-Qaeda. Due di essi si schiantarono contro il World Trade Center di New York, uno contro l'ala ovest del Pentagono a Washington, DC, e un altro, che si pensa si stesse dirigendo contro la Casa Bianca, fu eroicamente dirottato dai passeggeri, i quali morirono insieme ai terroristi quando l'aereo precipitò in un campo a 120 chilometri da Pittsburgh, in Pennsylvania.

I diciannove terroristi che erano saliti sugli aerei quel giorno stavano attuando un complotto orchestrato dal pakistano Khalid Sheik Mohammed, il quale fu catturato

nel 2003. L'indagine ufficiale che fu condotta in seguito dalla squadra di esperti nota come Commissione dell'11 settembre portò alla luce le informazioni e gli avvertimenti che i servizi segreti americani avevano ricevuto prima degli attacchi. Il dipartimento della Sicurezza interna promise solennemente che da quel momento in poi tutti i servizi segreti avrebbero condiviso le informazioni necessarie per consentire agli analisti di «connettere i punti» e prevenire così futuri piani di attacco terroristico.

Come contribuiscono i matematici a questo impegno? E che genere di metodi utilizzano per analizzare le reti terroristiche?

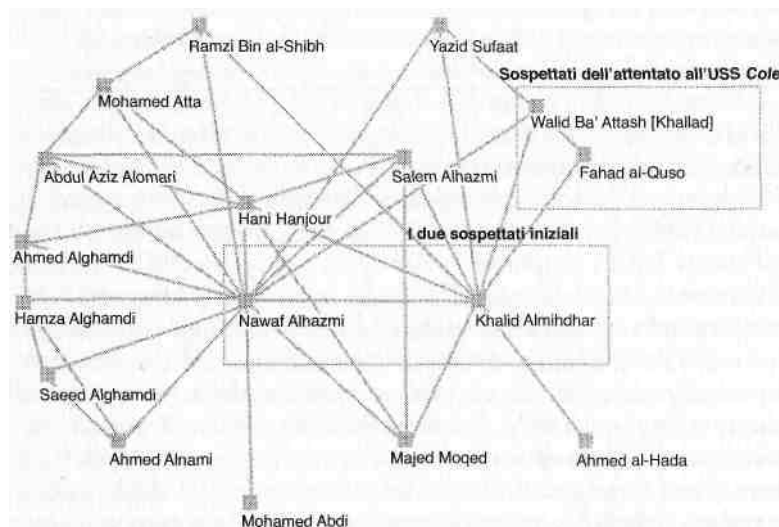
E difficile rendere giustizia alla vastità e al potere dei metodi matematici impiegati dai servizi segreti in quella che è divenuta nota come la «guerra al terrorismo». A dire il vero, descrivere tutte le tecniche usate non è soltanto difficile, ma è anche illegale: alcuni dei migliori lavori svolti dai matematici su questi problemi sono strettamente riservati.

La National Security Agency (NSA), ad esempio, che è nota per essere l'ente governativo che più si avvale del lavoro di ricercatori matematici, e organizzazioni affiliate, come i Centers for Communications Research (CRC), lavorano con gli esperti di *problem solving* più abili e creativi del mondo. Questi matematici sviluppano metodi altamente specializzati e li utilizzano per risolvere problemi reali negli ambiti della crittologia, dell'elaborazione di segnali e dati vocali, e del controterrorismo. La NSA e le organizzazioni affini mantengono anch'esse, per proprio conto, una rete estesa: una rete di matematici di varie università (compresi entrambi gli autori di questo libro) che di tanto in tanto lavorano con loro per aiutarle a mettere a punto nuovi metodi e a risolvere problemi difficili. (In uno dei primi episodi di *NUMB3RS*, l'agente dell'FBI Don Eppes rimane stupito quando scopre che suo fratello minore Charlie è stato consulente per la NSA e ha un nulla osta di segretezza di livello più alto del suo.)

Forse il modo migliore (e il più sicuro per noi due) per darvi un'idea di alcuni dei metodi impiegati è di prendere in considerazione studi che sono stati condotti da esperti esterni alle reti dei servizi segreti, utilizzando informazioni di pubblico dominio. Una delle analisi pubbliche più interessanti della rete terroristica coinvolta negli eventi dell'11 settembre fu divulgata nell'aprile 2002 tramite la rivista online *First Monday*. L'articolo, intitolato *Uncloaking Terrorist Networks*, era stato scritto da Valdis E. Krebs, un consulente gestionale con una buona preparazione matematica che in più occasioni aveva avuto modo di applicare l'analisi delle reti sociali per aiutare clienti quali IBM, Boeing e Price Waterhouse Coopers a capire come fluiscono le informazioni e come funzionano le relazioni nei sistemi umani complessi. Krebs aveva utilizzato alcuni calcoli standard della NSA per analizzare la struttura delle parti della rete di al-Qaeda che (come mostravano alcuni documenti di pubblico dominio) erano coinvolte nell'attacco dell'11 settembre. La figura 9 mostra un grafo delle relazioni tra alcuni dei soggetti chiave, secondo quanto riportato dall'articolo di Krebs e da un'analisi successiva pubblicata sul suo sito web (orgnet.com). Le linee indicano le connessioni dirette tra i terroristi sospettati nelle prime indagini iniziate nel gennaio del 2000, quando la CIA fu informata del fatto che due militanti di al-Qaeda, Nawaf Alhazmi e Khalid Almihdhar (indicati in uno

dei riquadri), erano stati fotografati mentre partecipavano a un incontro di noti terroristi in Malaysia, in seguito al quale erano ritornati a Los Angeles, dove vivevano dal 1999. Il secondo riquadro contiene il nome di Fahad al-Quso, la cui connessione con Almihdhar fu stabilita quando entrambi parteciparono all'incontro in Malaysia. Al-Quso e Walid Ba' Attash entrarono in seguito nella lista dei sospetti per l'attentato del 12 ottobre 2000 contro il cacciatorpediniere americano USS *Cole* nel porto yemenita di Aden, in cui morirono diciassette marinai. Nella rete mostrata nella figura 9 si trovano anche undici dei diciannove terroristi dell'11 settembre, che sono tutti collegati direttamente o indirettamente ad Almihdhar e ad Alhazmi, i sospetti originari.

Figura 9. Schema della rete dei membri di al-Qaeda coinvolti nell'attentato dell'11 settembre.



Naturalmente, questo grafo di rete fu disegnato «dopo i fatti» dell'11 settembre e le indagini che seguirono. La principale sfida per gli investigatori - e quindi per i matematici - è ricavare le informazioni in anticipo, per lo più da quadri molto più vasti, comprendenti centinaia o addirittura migliaia di individui. Queste grandi reti possono facilmente portare a molte false piste. Normalmente esse sono anche soggette al fastidioso fenomeno dei dati mancanti, come nomi di membri importanti di cui non è nota l'esistenza, e che pertanto non figurano nel grafo, oppure che sono presenti ma senza che se ne conoscano le connessioni con gli altri individui.

Un lavoro assai difficile, ma molto importante, è identificare in una grande rete gli individui che svolgono ruoli chiave in qualità di capi, facilitatori, intermediari e così via. Gli strumenti matematici della teoria dei grafi e dell'analisi delle reti sociali possono essere applicati per identificare questi individui. Ad esempio, analizzando un grafo di rete più grande nel suo articolo del 2002, Krebs elaborò tre «classifiche» pensate in modo da rivelare chi erano gli individui più importanti nella rete. In ciascuna delle tre classifiche, i primi cinque individui erano i seguenti:

Grado di centralità locale	Grado di intermediazione	Grado di centralità globale
Mohamed Atta	Mohamed Atta	Mohamed Atta
Marwan al-Shehhi	Essid Sami Ben Khemais	Marwan al-Shehhi
Hani Hanjour	Zacarias Moussaoui	Hani Hanjour
Essid Sami Ben Khemais	Nawaf Alhazmi	Nawaf Alhazmi
Nawaf Alhazmi	Hani Hanjour	Ramzi Bin al-Shibh

In cima a tutte e tre le classifiche si trovava Mohamed Atta, l'uomo che Osama bin Laden aveva riconosciuto come leader del complotto dell'11 settembre in una famosa videoregistrazione diffusa poco dopo gli attacchi. Altri, come Alhazmi, uno dei due sospetti originari, Hanjour e al-Shehhi erano tra i diciannove terroristi che erano saliti sugli aerei l'11 settembre e che erano morti quel giorno. Altri ancora non erano saliti sugli aerei ma avevano svolto ruoli chiave: Moussaoui, in seguito condannato come il «ventesimo dirottatore», Bin al-Shibh, compagno di stanza di Atta in Germania che non era riuscito a ottenere il visto d'ingresso per gli Stati Uniti, e Ben Khemais, capo della rete logistica europea di al-Qaeda, in seguito condannato a Milano con l'accusa di cospirazione in un altro complotto.

Il fatto che questi individui chiave fossero stati selezionati a partire da un grafo di rete molto più grande di quello illustrato sopra, utilizzando i metodi standard di analisi delle reti sociali, mostra l'utilità di tali calcoli, che vengono attualmente eseguiti migliaia di volte al giorno da sistemi informatici programmati per aiutare gli analisti a monitorare le reti terroristiche.

Teoria dei grafi e «misure di centralità»

Per comprendere i calcoli utilizzati per selezionare gli individui chiave nel grafo di rete, dobbiamo mettere insieme alcune idee fondamentali. Prima di tutto, il concetto matematico di «grafo» usato in questo contesto differisce dal concetto comune di «grafico», come il grafico di una curva in un piano cartesiano. Esso si riferisce piuttosto a un insieme di punti chiamati «nodi» - persone, ad esempio - alcuni dei quali sono connessi da linee, chiamate «spigoli», mentre altri sono privi di collegamento. I grafi semplici, nei quali non sono consentite connessioni multiple tra gli stessi due nodi, sono usati per rappresentare l'esistenza di qualche relazione, come «lavora con», «ha un legame con» o «si sa che ha comunicato con». Se due nodi non sono connessi da uno spigolo, significa che tra di essi quella relazione non esiste, o non è nota.

I disegni dei grafi sono utili, ma lo stesso grafo può essere rappresentato da molte immagini, giacché la posizione dei nodi viene scelta per ragioni di pura comodità (o per ragioni estetiche). Da un punto di vista matematico, un grafo non è un disegno, bensì un insieme astratto di nodi (chiamati anche «vertici») e di spigoli che

connettono tra loro alcune coppie di nodi.

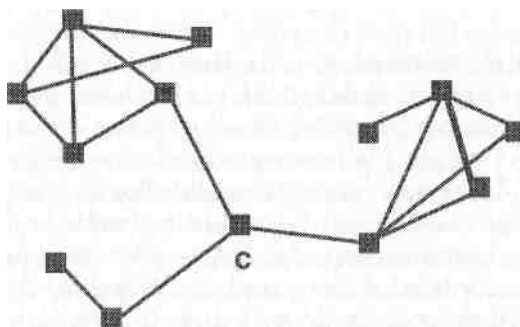
Un concetto fondamentale della teoria dei grafi che si rivela importante nell'analisi delle reti sociali è la centralità locale di un nodo, vale a dire il numero di altri nodi con cui è connesso direttamente da spigoli. In un grafo che descrive una rete di uomini, i nodi con un'elevata centralità locale rappresentano gli individui «ben connessi», per lo più i capi.

Ma le connessioni dirette non sono l'unica cosa che conta. Un altro concetto importante è la «distanza» tra due nodi. Si dice che due nodi qualsiasi A e B sono connessi (anche indirettamente) se esiste qualche percorso che va da A a B, cioè se esiste qualche sequenza di nodi che inizia con A e termina con B, nella quale ciascun nodo è connesso a quello successivo da uno spigolo. In altre parole, un percorso è un cammino tra due nodi in cui si procede lungo gli spigoli, usando i nodi intermedi come «pietre di guado» su cui appoggiare il piede. La lunghezza di un percorso è il numero di spigoli che contiene e il percorso più breve possibile tra due nodi A e B è la loro distanza, denotata con il simbolo $d(A,B)$. Questi percorsi di lunghezza minima sono chiamati «percorsi geodetici». In particolare, ogni spigolo è un percorso geodetico di lunghezza 1.

Il concetto di distanza tra due nodi conduce a un altro modo di identificare i nodi chiave, cioè porta ad altre misure di centralità, le quali possono essere utilizzate per attribuire a ciascun nodo un «punteggio» che suggerisce qualcosa sulla sua potenziale importanza. Il concetto di «intermediazione» attribuisce a ogni nodo un punteggio che riflette il suo ruolo come pietra di guado lungo i percorsi geodetici tra altre coppie di nodi. L'idea è che se un percorso geodetico da A a B (ce ne possono essere più di uno) passa per C, allora C acquista una potenziale importanza. Più nello specifico, l'intermediazione di C come collegamento tra A e B è definita come:

$$\frac{\text{il numero di percorsi geodetici da A a B che passano per C}}{\text{diviso per}} \quad \text{il numero di percorsi geodetici da A a B.}$$

Il punteggio complessivo di intermediazione di C si ottiene sommando i risultati di questi calcoli per tutte le possibili coppie di nodi A e B. Qui sotto vediamo l'esempio di un nodo con bassa centralità locale ma alta intermediazione:



Tali nodi - o le persone che rappresentano in una rete umana - possono avere un ruolo importante nel collegare tra loro insiemi di nodi che avrebbero altrimenti poche altre connessioni, se non nessuna.

La terza «misura di centralità» usata da Krebs, e mostrata nella tabella che abbiamo visto prima, è la misura di centralità globale. In parole povere, essa indica quanto ciascun nodo sia vicino agli altri nodi nel grafo. Per un dato nodo C, prima si calcolano le distanze $d(C,A)$, $d(C,B)$, e così via, da tutti gli altri nodi del grafo. Poi si sommano tra loro gli inversi di queste distanze, cioè si calcola la somma:

$$1 / d(C,A) + 1 / d(C,B) + \dots$$

Minore è la distanza tra C e un altro nodo, maggiore sarà l'inverso di questa distanza. Ad esempio, se C ha 10 nodi a distanza 1 (il che significa che ha una centralità locale pari a 10), si inizia il calcolo della centralità globale sommando 1 dieci volte. Se ci sono altri 60 nodi a distanza 2 da C, si somma $1/2$ 60 volte, e se ci sono 240 nodi a distanza 3 da C, si somma $1/3$ 240 volte:

$$10 \times 1 + 60 \times 1/2 + 240 \times 1/3 \dots = 10 + 30 + 80$$

Mentre le misure di centralità locale considerano soltanto i nodi immediatamente adiacenti, la centralità globale tiene conto anche dei nodi a distanza 2, 3 e così via. Gli analisti considerano la centralità globale un buon indice della velocità con cui le informazioni possono diffondersi tra i nodi di una rete.

Grafi casuali: strumenti utili per comprendere grandi reti

La quantità di informazioni dettagliate contenuta in un grande grafo, come quelli creati dalla NSA per monitorare le comunicazioni telefoniche o gli scambi di messaggi elettronici in regioni come il Medio Oriente, è talmente grande che i matematici, per ovvie ragioni, desiderano trovare «modelli ridotti», cioè grafi simili che siano abbastanza piccoli da poter essere studiati e compresi in tutte le loro caratteristiche, e che possano poi fornire suggerimenti in merito a che cosa cercare quando si analizzano i veri grafi. Ricerche recenti sui grafi e sulle reti hanno condotto a un interesse sempre più diffuso per quelli che vengono chiamati grafi casuali. Questi grafi possono essere utili non solo per comprendere le caratteristiche strutturali dei grafi e delle reti di grandi dimensioni, ma anche per stimare quante informazioni manchino in un grafo costruito sulla base di dati incompleti. Dal momento che è pressoché impossibile ottenere dati completi sulle comunicazioni e sulle relazioni tra le persone comprese in una rete - soprattutto in una rete segreta - questo genere di stime riveste un'importanza cruciale.

La scintilla che fece sorgere l'interesse per lo studio dei grafi casuali fu una ricerca condotta nei tardi anni '50 dai matematici ungheresi Paul Erdős e Alfred Renyi. Quelli che essi studiarono erano modelli piuttosto semplici di grafi casuali. Il più importante era strutturato in questo modo:

Si prenda un certo numero di nodi n . Per ogni coppia di nodi - ci sono

$n \times (n - 1)/2$ coppie - si decida se i due nodi siano o meno connessi da uno spigolo mediante un esperimento casuale: nello specifico, si lanci una moneta che ha probabilità p di dare testa come risultato e si inserisca uno spigolo ogni volta che l'esito del lancio è testa.

Così, l'esistenza di ogni spigolo è determinata dal caso, e la sua comparsa o meno è del tutto indipendente dalla presenza o assenza degli altri spigoli. Data la sua costruzione casuale, si potrebbe pensare che c'è poco da dire su un grafo del genere, ma è vero proprio il contrario. Lo studio dei grafi casuali si è dimostrato di grande utilità, in particolare nell'aiutare i matematici a comprendere l'importante concetto strutturale di quelle che vengono chiamate le componenti di un grafo. Se da ogni nodo di un grafo ha origine un percorso che conduce a tutti gli altri nodi, si dice che il grafo è connesso. In caso contrario, i nodi del grafo possono essere suddivisi in due o più componenti, ovvero insiemi di nodi tali per cui tutte le coppie di nodi di un dato insieme sono connesse da qualche percorso ma non esistono percorsi che connettono i nodi di due componenti diverse (questo è un modo dei matematici di descrivere il fenomeno dell'«impossibilità di andare da qui a lì»).

Erdős e Renyi dimostrarono che i valori di p vicini a $1/n$ sono critici per la determinazione delle dimensioni e del numero di componenti in un grafo casuale. (Si noti che, in media, ciascun nodo sarà connesso da uno spigolo a un numero di altri nodi pari a $[n-1] \times p$. Quindi se il valore di p è vicino a $1/n$ la misura media di centralità locale di tutti i nodi sarà circa 1.) Nello specifico, Erdős e Renyi dimostrarono che se il numero di spigoli è inferiore al numero di nodi di qualche percentuale, il grafo tenderà a essere scarsamente connesso - con un numero molto grande di componenti - mentre se il numero di spigoli è superiore al numero di nodi di qualche percentuale, il grafo conterrà probabilmente una componente gigante composta da una cospicua frazione di nodi e una seconda componente, in ordine di dimensioni, molto più piccola della prima. Il perfezionamento di questi risultati è ancora oggetto di interessanti ricerche matematiche.

Tra la fine degli anni '90 e l'inizio del 2000 lo studio dei grafi casuali ha visto un'esplosione di interesse da parte sia dei matematici puri sia degli analisti delle reti sociali. Ciò si deve in gran parte alla presa di coscienza del fatto che esistono modelli probabilistici molto più flessibili e realistici per i tipi di grafi che si osservano nelle reti reali.

Dato che le reti reali sono in costante evoluzione e trasformazione, lo studio matematico dei grafi casuali si è concentrato sui modelli che descrivono la crescita dei grafi. In un fondamentale articolo scritto nel 1999, Albert Barabasi e Reka Albert proposero un modello di collegamento preferenziale, nel quale nuovi nodi vengono aggiunti a un grafo e hanno una quota fissa di spigoli che sono connessi in modo casuale ai nodi preesistenti con probabilità proporzionali alla centralità locale di questi ultimi. Questo modello ebbe un successo sorprendente nel descrivere un grafo molto importante, cioè il grafo che rappresenta i siti web (i nodi) e i loro collegamenti (le connessioni tra i nodi). Esso riuscì anche a fornire un meccanismo per generare grafi in cui la frequenza di nodi con misure di centralità locale differenti segue una *distribuzione a legge di potenza*, vale a dire in cui la quantità di nodi con centralità

locale n è all'incirca proporzionale a $1/n^3$. Ricerche successive hanno portato a metodi di costruzione di grafi casuali «in crescita» con potenze arbitrarie come $n^{2,4}$ o $n^{2,7}$ al posto di n^3 . Tali metodi possono essere utili per modellizzare le reti reali.

Sei gradi di separazione: «Com'è piccolo il mondo!»

Un'altra linea di ricerca in ambito matematico che ha recentemente attratto l'attenzione degli analisti di reti è chiamata il «modello del mondo piccolo». Il catalizzatore fu un articolo del 1998 di Duncan Watts e Steven Strogatz, in cui i due autori dimostravano che l'introduzione in una grande rete di poche connessioni casuali a lunga distanza tende a ridurre drasticamente il diametro della rete, cioè la distanza più grande tra i nodi che la compongono. Queste «scorciatoie temporanee» sono spesso presenti nelle reti reali; infatti, l'analisi di Krebs della rete terroristica coinvolta negli eventi dell'11 settembre descriveva, a ragion veduta, gli incontri avvenuti in momenti precisi tra i rappresentanti di rami distanti della rete di al-Qaeda per coordinare i lavori e riferire i progressi nella preparazione degli attacchi.

Lo studio più famoso di questo fenomeno fu pubblicato nel 1967 dallo psicologo sociale Stanley Milgram, il quale suggeriva che se si fossero presi a caso due cittadini statunitensi, in media essi sarebbero risultati connessi da una catena di conoscenti composta da sei individui. A sostanziare la teoria di Milgram era un esperimento nel quale aveva ingaggiato sessanta persone a Omaha, in Nebraska, e aveva affidato loro il compito di recapitare (a mano!) delle lettere a un agente di cambio del Massachusetts servendosi di intermediari potenzialmente connessi al destinatario attraverso una catena di «amici di amici di amici». In realtà, soltanto tre dei cinquanta tentativi compiuti raggiunsero l'obiettivo, ma la novità e il fascino dell'esperimento e dell'idea che lo aveva ispirato gli garantirono una fama duratura.

Il lavoro più consistente realizzato da Watts e Strogatz portò a ricerche più precise e utili, ma l'idea dei «sei gradi» guadagnò una notorietà tale che nel pensiero comune su questa materia il mito per lo più domina sui fatti. L'espressione «sei gradi di separazione» fu coniata nel titolo di un'opera teatrale di John Guare del 1991, nella quale una donna dice a sua figlia: «Tutti su questo pianeta siamo separati soltanto da altre sei persone [...] Io sono collegata, tu sei collegata, a chiunque altro sulla Terra da una catena di sei persone. E un pensiero profondo». Non è vero, ma è un'idea affascinante.

Quello che in realtà sembra vero è che i diametri delle reti - le lunghezze maggiori (o medie) dei percorsi tra i nodi - sono più piccoli di quanto ci si aspetterebbe basandosi soltanto sulle loro dimensioni. Ci sono due esempi interessanti di cui si parla molto in campi completamente diversi. In ambito cinematografico, il «gioco di Kevin Bacon» riguarda le connessioni tra gli attori dei film. Utilizzando gli attori come nodi di un grafo, si considerano due attori connessi da uno spigolo se hanno recitato insieme almeno in un film. Dato che Kevin Bacon è apparso nei film assieme a moltissimi altri attori, l'idea è nata qualche anno fa per mostrare che due attori non sono molto distanti in questo grafo se entrambi hanno un piccolo «numero di Bacon»,

definito come la loro distanza geodetica da Kevin Bacon. Quindi, un attore che è apparso in un film con Kevin Bacon avrà un numero di Bacon pari a 1, un attore che non ha mai recitato con lui ma che è apparso in un film con un altro attore avente numero di Bacon 1 avrà un numero di Bacon pari a 2, e così via. Uno studio recente ha prodotto la seguente distribuzione dei numeri di Bacon:

0	1	2	3	4	5	6	7	8
1	1673	130.851	349.031	84.615	6718	788	107	11

La distanza media da Kevin Bacon di tutti gli attori compresi nello studio era 2,94. Di conseguenza, una stima in difetto della distanza tra due attori qualsiasi (ottenuta sommando le loro distanze da Kevin Bacon) sarà circa 2 per 2,94, cioè circa 6! Naturalmente questa stima è in difetto (Kevin Bacon potrebbe non trovarsi nel percorso più breve tra due attori) e manca anche di soddisfare il principio dei «sei gradi di separazione» per il grafo degli attori di uno stesso film, dal momento che alcuni di essi hanno già una distanza da Kevin Bacon maggiore di 6. (Naturalmente, gli attori conoscono molti altri attori con cui non sono mai apparsi in un film.)

I matematici hanno un altro eroe: lo stesso Paul Erdős che abbiamo incontrato prima. Nel corso della sua vita, Erdős fu autore di più di 1500 articoli scritti con più di 500 coautori, fatto che lo rese uno dei matematici più prolifici del XX secolo. Nel 2000, utilizzando i dati relativi ad articoli di matematica usciti su riviste specialistiche nell'arco di sessant'anni, Jerrold Grossman ha costruito un «grafo di collaborazioni tra matematici» con 337.454 nodi (autori) e 496.489 spigoli che connettevano gli autori che avevano scritto almeno un articolo insieme. La centralità locale media in questo grafo era 3,92 e infatti in esso si trovava una «componente gigante» comprendente 208.200 vertici, mentre i rimanenti 45.139 vertici erano suddivisi tra altre 16.883 componenti. Il «numero di Erdős» di un matematico è la distanza più breve tra lui e Paul Erdős. Per convenzione, questo numero è 0 per lo stesso Erdős, 1 per gli oltre 500 matematici che hanno scritto un articolo con lui, 2 per quelli che hanno scritto almeno un articolo con uno dei coautori di Erdős e così via. (Entrambi gli autori di questo libro hanno un numero di Erdős 2; Devlin in realtà una volta ha scritto un articolo con Erdős che però non conta perché non è mai stato pubblicato.) Ai tempi dello studio di Grossman, il numero di Erdős medio per tutti i matematici che avevano pubblicato qualche articolo era 4,7. Il più grande numero di Erdős conosciuto è 15.

Un esempio di connessione dei punti riuscita

Uno degli obiettivi degli analisti di reti sociali è valutare quali siano gli spigoli mancanti in un grafo costruito a partire da informazioni incomplete. Ad esempio, il «problema della triade» riguarda il fenomeno della «triangolarità». Se A, B e C sono tre nodi di una rete e si sa che esiste una determinata relazione tra A e B e tra A e C, allora c'è qualche possibilità che la stessa relazione - magari «conosce» o «comunica con» o «lavora con» - sussista anche tra B e C. Tale possibilità è meglio espressa in

termini di probabilità, e i matematici cercano di stabilire come fare a stimare tali probabilità sulla base di tutte le informazioni disponibili. Per particolari tipi di reti e di relazioni, le informazioni dettagliate sulle connessioni tra A e B e tra A e C possono essere usate per fare ipotesi razionali sulla probabilità di una relazione tra B e C. Tali ipotesi possono essere combinate con altre fonti di informazioni su una rete in un modo che accresce la capacità di un analista di identificare i nodi chiave, ovvero quelli che meriteranno la massima attenzione nelle future operazioni di sorveglianza.

Il 7 giugno 2006, durante un incontro in un rifugio isolato vicino a Baqubah, in Iraq, Abu Musab al-Zarqawi, il leader di al-Qaeda in Iraq e il terrorista più ricercato in quella zona di guerra, è stato ucciso dalle bombe sganciate dai caccia F-16 americani. Localizzare e uccidere al-Zarqawi, che aveva guidato una pericolosa campagna terroristica nel corso della quale alcuni civili americani che lavoravano in Iraq erano stati presi in ostaggio e decapitati, era da molti anni un obiettivo di massima priorità dei governi statunitense, iracheno e giordano. Di conseguenza, era stata impegnata una grande quantità di energie e di lavoro nell'impresa di rintracciarlo.

Sebbene i dettagli dei metodi impiegati siano strettamente riservati, è noto che i movimenti e le comunicazioni di una grande rete di complici di al-Zarqawi erano stati monitorati il più da vicino possibile per molto tempo. Uno di questi complici, Sheik Abdul Rahman, definito il «consigliere spirituale» di al-Zarqawi, era stato individuato e alla fine aveva fornito l'anello di collegamento critico. Come ha affermato il portavoce dell'esercito degli Stati Uniti, il generale maggiore William Caldwell,

attraverso il minuzioso lavoro dei servizi segreti, abbiamo potuto iniziare a seguire le sue [di Abdul Rahman] tracce, a monitorare i suoi spostamenti e a stabilire quando entrava in contatto con al-Zarqawi [...] è stato davvero un lungo, scrupoloso e ponderato utilizzo dei servizi segreti, del lavoro di raccolta informazioni, delle risorse umane ed elettroniche e dell'analisi delle radiocomunicazioni, durato molte, molte settimane.

Si può solo provare a immaginare che aspetto potessero avere i grafi di rete costruiti dagli analisti dei servizi segreti statunitensi, ma evidentemente il passaggio chiave era stato identificare e concentrarsi su un nodo situato a distanza 1 dal bersaglio più importante.

IL DILEMMA DEL PRIGIONIERO, L'ANALISI DEL RISCHIO E IL CONTROTERRORISMO

Nella prima serie di *NUMB3RS*, un episodio intitolato *Pericolo in città*, trasmesso in Italia il 24 giugno 2007, delineava uno scenario terroristico molto reale, e spaventoso: la minaccia di far esplodere una «bomba sporca», contenente materiale radioattivo associato a una carica esplosiva convenzionale, con l'intento di disperdere il letale materiale radioattivo in una vasta area. Nell'episodio, una banda di terroristi locali dirotta un autocarro che trasporta canister di cesio-137, un isotopo radioattivo. Grazie a una svolta nelle indagini, l'FBI riesce a fare irruzione nel nascondiglio dei criminali e tre membri della banda vengono arrestati. Sfortunatamente, però, l'FBI non riesce a trovare né l'autocarro né il materiale radioattivo, e almeno uno dei cospiratori rimane a piede libero. I tre uomini arrestati minacciano le autorità affermando che, se non verranno rilasciati, faranno esplodere a Los Angeles la bomba che dicono di aver costruito.

Don e i suoi colleghi dell'FBI interrogano i sospetti con i metodi convenzionali, cioè separandoli e cercando di fare in modo che ognuno di loro riveli dove si trova l'autocarro, in cambio di un patteggiamento della pena. Ma i tre hanno un'altra idea e dicono che riveleranno dove si trova l'autocarro solo *dopo* essere stati rilasciati. Don chiede a Charlie di aiutarlo a superare questa situazione di stallo.

Charlie vede la possibilità di utilizzare un classico problema matematico, il «dilemma del prigioniero», dalla branca della matematica chiamata teoria dei giochi. Charlie spiega il problema nella sua forma canonica, che coinvolge solo due prigionieri:

Supponiamo che due persone abbiano commesso un crimine. Se nessuno dei due confessa, entrambi sono condannati a una pena di un anno. Se soltanto uno dei due confessa, quello che ha parlato è libero, mentre l'altro è condannato a una pena di cinque anni. Se confessano tutti e due, sono condannati entrambi a una pena di due anni.

Una possibile base logica di questo scenario è la seguente: se solo uno dei due prigionieri confessa, sarà liberato come ricompensa per la sua promessa di testimoniare al processo contro l'altro prigioniero, il quale invece sarà condannato alla sentenza piena di cinque anni. Se nessuno dei due confessa, sarà più difficile dimostrare la colpevolezza dei due sospetti e gli avvocati difensori patteggeranno una pena di un anno. Se entrambi i prigionieri confessano, tutti e due saranno condannati a una pena di due anni, anziché di cinque, come ricompensa per la loro cooperazione,

che consente di evitare un processo.¹⁸

Questo scenario pone un serio dilemma. Il peggior risultato complessivo per entrambi i prigionieri si ha nel caso in cui tutti e due confessino; se lo fanno, sono entrambi condannati a una pena di due anni. Quindi, per ognuno, sembrerebbe ragionevole tacere, e scontare un anno anziché due. Ma se foste uno dei prigionieri, e aveste concluso che è meglio restare in silenzio e scontare una pena di un anno, non sareste tentati di cambiare idea all'ultimo momento e di tradire il vostro compagno, in modo da farla franca? Sembrerebbe una mossa furba, giusto? In effetti, sarebbe stupido non farlo. Il problema è che il vostro compagno sicuramente ragionerà allo stesso modo e che, di conseguenza, entrambi finirete per trascorrere due anni in prigione. Più ci si pensa, più ci si ritrova in un circolo vizioso. Alla fine, dovrete arrendervi all'idea di non avere alternative se non quella di compiere la stessa azione che, come entrambi sapete, condurrà al peggior risultato.

Se non siete ancora convinti del fatto che questo problema è davvero senza soluzione, andate avanti a leggere. Come Charlie, considereremo il problema da un punto di vista matematico e trarremo una risposta concreta.

La teoria dei giochi

La teoria dei giochi divenne una disciplina matematica nel 1994 con la pubblicazione del libro di John von Neumann e Oskar Morgenstern *The Theory of Games and Economic Behavior*. Il loro modo di definire il gioco che Charlie sta descrivendo è nei termini di una matrice dei profitti (*pay of matrix*) come questa:

		Strategia del prigioniero n. 2	
		Non Confessa	Confessa
Strategia del prigioniero n. 1	Non confessa	Entrambi sono condannati a 1 anno	N. 1 è condannato a 5 anni
	Confessa	N. 2 è condannato a 5 anni	Entrambi sono condannati a 2 anni

Si noti che in tutti i casi in cui un prigioniero confessa e l'altro no, quello che confessa è libero mentre l'altro, il prigioniero che ha scelto di non tradire il compagno, viene condannato a una pena di cinque anni.

Vediamo ora se riusciamo a capire quale sia la strategia migliore per il prigioniero n. 1 (per il prigioniero n. 2 vale esattamente la stessa analisi).

Una strategia è definita «dominata» se conduce a risultati peggiori di un'altra strategia indipendentemente da quello che fa l'altro giocatore. Se una strategia è dominata, l'altra strategia dovrebbe essere una scelta migliore, giusto? Vediamo.

Se foste il prigioniero n. 1, fareste sempre meglio a confessare. Se anche il vostro

¹⁸ Continueremo a spiegare il problema mantenendo i numeri indicati, anche se, in realtà, quello che conta non sono i numeri effettivi (uno, due, cinque anni), ma solo il *rapporto tra i numeri*.

compagno confessasse, sareste condannati a una pena di due anni anziché di cinque; se il vostro compagno non confessasse, vi guadagnereste la libertà al posto di una pena di un anno. Quindi «non confessare» è una strategia dominata e «confessare» è una scelta migliore, indipendentemente da quello che fa l'altro! (La teoria dei giochi si basa sul presupposto che entrambi i giocatori siano razionali ed egoisti, e che la matrice dei profitti sia l'unica cosa che conta. Pertanto, a meno che i profitti non includano in qualche modo un «costo del tradimento di un compagno», come può accadere, il nostro ragionamento non fa una piega.)

Ma non è finita qui. Si noti che se entrambi i prigionieri adottano la strategia migliore, il risultato è che tutti e due dovranno scontare una pena di due anni, mentre se entrambi impiegano la strategia peggiore, «non confessare», il risultato è per tutti e due una pena inferiore, di solo un anno. Allora ciò che è meglio per ogni singolo giocatore non è la cosa migliore per i giocatori presi collettivamente. Qui entra in gioco il fenomeno che gli studiosi della teoria dei giochi chiamano cooperazione. Se i prigionieri cooperano tra loro, e non si tradiscono l'un l'altro, *allora* otterranno il miglior risultato possibile.

Questo apparente paradosso - il conflitto tra il proprio interesse razionale e ciò che può essere raggiunto attraverso la cooperazione - ha avuto una profonda influenza sullo sviluppo della teoria dei giochi nella seconda metà del XX secolo. Lo stesso dilemma del prigioniero fu originariamente proposto da due matematici, Merrill Flood e Melvin Dresher, alla RAND Corporation, una commissione governativa di esperti che furono tra i primi a sperimentare l'applicazione di metodi matematici alle strategie del governo statunitense. La teoria dei giochi fu uno strumento importante per le strategie militari durante la guerra fredda e, come vedremo, svolge ancora un ruolo di rilievo nelle analisi matematiche delle strategie adottate nella guerra contro il terrorismo.

John Nash, il geniale matematico affetto da disturbi mentali rappresentato nel film *A Beautiful Mind*, vinse un premio Nobel per l'economia grazie al fondamentale contributo che diede alla teoria dei giochi durante il suo dottorato di ricerca in matematica alla Princeton University. La sua teoria, che riguardava quelli che oggi vengono chiamati equilibri di Nash, aveva a che fare con le strategie «di cui non ci si può pentire», vale a dire combinazioni di scelte strategiche da parte dei singoli giocatori di cui nessun giocatore potrà mai pentirsi dicendo «avrei fatto meglio invece a adottare la strategia X». Per qualunque gioco con due o più giocatori, ciascuno con una lista finita di strategie possibili, Nash dimostrò che esiste almeno un equilibrio di questo tipo: almeno una combinazione di strategie per i giocatori che è stabile nel senso che nessun giocatore può ottenere un profitto migliore cambiando strategia se nessun altro la cambia.

L'idea di Nash era che in un gioco in cui tutti i giocatori sono razionali ed egoisti, cioè interessati soltanto a massimizzare il proprio profitto personale, gli unici risultati stabili possibili sono questi equilibri, dal momento che per tutte le altre combinazioni di scelte strategiche almeno un giocatore potrebbe ottenere un profitto maggiore cambiando strategia. Spesso questi equilibri coinvolgono quelle che gli studiosi della teoria dei giochi chiamano «strategie miste», nelle quali ciascun giocatore può adottare più di una delle strategie comprese nella sua lista (le cosiddette strategie

pure), a condizione che assegni una probabilità a ognuna e scelga una strategia pura a caso in base a queste probabilità. Nella guerra di cervelli («gioco di strategia») tra un lanciatore e un battitore nel baseball, ad esempio, il lanciatore potrebbe scegliere tra le strategie pure di palla veloce, palla curva e cambio di velocità con probabilità del 60 per cento, del 33 per cento e del 7 per cento in modo che il battitore sia continuamente costretto a indovinare.

Nella matrice dei profitti mostrata per il dilemma del prigioniero, esiste solo una combinazione di strategie che porta a un equilibrio di Nash, ed è una combinazione di due strategie pure: entrambi i prigionieri scelgono di «confessare». Se uno dei due prigionieri cambia strategia senza che lo faccia anche l'altro, la sua pena aumenta da due a cinque anni. Ma se *tutti e due* cambiano strategia, entrambi ricaveranno un profitto maggiore, riducendo la pena da due anni a uno.

Provaci ancora, Sam

Il dilemma del prigioniero e altri paradossi simili hanno contribuito a stimolare lo sviluppo di formulazioni matematiche più generali, come l'idea che, giocando ripetutamente allo stesso gioco, due giocatori possano imparare a cooperare sperimentando come la collaborazione porti a profitti migliori. Ciò conduce a possibilità interessanti, e in un famoso esperimento condotto attorno al 1980 il matematico e politologo Robert Axelrod, dell'Università del Michigan, organizzò un torneo invitando colleghi di tutto il mondo a realizzare programmi informatici che dovevano poi scontrarsi in una serie di partite basate sul dilemma del prigioniero, senza alcun «accordo» o comunicazione di intenti preventiva. Il programma di ogni concorrente poteva fare assegnamento soltanto sul modo in cui il programma dell'avversario stava giocando la partita.

Il vincitore del torneo fu stabilito semplicemente segnando i punti: qual era il profitto medio vinto da ciascun programma contro tutti gli altri? Sorprendentemente, vinse il più semplice di tutti i programmi in gara: il programma Tit for Tat di Anatol Rapoport. Esso si comportava secondo la seguente regola: scegliere la strategia «cooperare» nella prima partita, e nelle partite successive adottare la strategia che l'altro giocatore ha scelto nella partita precedente. Questo programma non è né troppo buono - punirà immediatamente l'altro giocatore per aver scelto la strategia «tradire» - né troppo cattivo, in quanto continuerà a cooperare finché lo farà l'altro giocatore. Anche senza il privilegio della comunicazione tra i giocatori, la strategia *tit for tat* sembra indurre l'altro «giocatore» computerizzato a giocare nel suo stesso modo, portando al miglior risultato possibile per entrambi.

Nello scenario fittizio rappresentato nell'episodio di *NUMB3RS*, *Pericolo in città*, chiaramente *c'era stata* una comunicazione preventiva fra i tre criminali, i quali evidentemente avevano deciso di comune accordo che se fossero stati arrestati avrebbero dovuto tener duro e non confessare, convinti che questo atteggiamento avrebbe costretto l'FBI a rilasciarli al fine di prevenire la catastrofe radioattiva. Deviazioni simili dagli ordinari presupposti della teoria dei giochi vengono utilizzate

nei lavori che i matematici stanno attualmente compiendo per analizzare e prevedere le strategie dei terroristi e per stabilire quali siano le strategie migliori per difendersi dai loro attacchi. Un modo di applicare altre nozioni matematiche per perfezionare la teoria dei giochi è in realtà lo stesso metodo che Charlie impiega per convincere i criminali a violare il loro patto, e che vediamo adesso.

Valutazione del rischio

L'idea che sta dietro alla valutazione del rischio (talvolta chiamata «analisi del rischio» o «gestione del rischio») è che un individuo, o un gruppo, posto dinanzi a possibili perdite può assegnare a ogni perdita un valore numerico - magari effettivi costi monetari - e, considerando il costo e la probabilità di ciascuna perdita, stabilire la perdita o il rischio previsti che essa rappresenta. Si possono quindi considerare linee di azione in grado di ridurre i rischi, per quanto possano anch'esse comportare qualche costo. L'obiettivo generale è trovare la migliore combinazione di azioni capace di minimizzare il costo complessivo: quello delle azioni più i rischi che rimangono dopo che esse sono state compiute.

Una delle prime applicazioni dell'analisi del rischio furono i calcoli effettuati dalle agenzie di assicurazioni per stabilire quanto denaro dovessero aspettarsi di pagare ogni anno per risarcire i clienti che presentavano domanda e la probabilità che l'insieme complessivo delle domande di indennizzo eccedesse le riserve finanziarie. Allo stesso modo, molte aziende e agenzie governative eseguono valutazioni matematiche di rischi di vario tipo - ad esempio quelli associati a disastri naturali come incidenti catastrofici, incendi, alluvioni e terremoti - e adottano misure come comprare polizze assicurative e installare attrezzature di sicurezza in modo da ridurre questi rischi in maniera efficace dal punto di vista economico.

Valutazioni dei rischi possono essere compiute anche nel sistema giudiziario penale, e di fatto vengono effettuate abitualmente dagli imputati, dai loro difensori e dagli avvocati dell'accusa, anche se di solito senza poter beneficiare dell'aiuto della vera matematica. Quello che Charlie capisce quando viene a trovarsi di fronte alla versione dell'FBI del dilemma del prigioniero - come fare a violare la solidarietà della strategia «nessuno parli» adottata dai criminali arrestati - è che la strategia comune espone i tre uomini a rischi molto diversi. Quando Don si lamenta con Charlie del fatto che nessuno sembra mostrare alcuna volontà di parlare, Charlie risponde: «Forse è perché nessuno di loro si rende conto di quanto gli altri abbiano da perdere».

Charlie convince Don a tentare un approccio diverso: portare i tre uomini in una stanza e presentare loro una valutazione matematica dei rischi in cui ciascuno incorre (nel senso della teoria dei giochi) andando in prigione. Dal momento che tutti e tre hanno - in un modo o nell'altro - una probabilità non trascurabile di andare in prigione per aver partecipato al complotto dell'arma radiologica, Charlie vuole mostrare loro quanto sarebbero diverse le conseguenze per ognuno preso individualmente.

Sebbene sia intimorito da questi uomini - che non assomigliano affatto al suo consueto uditorio di volenterosi studenti del CalSci - Charlie va avanti coraggiosamente, mormorando: «Quello che farò oggi, con qualche calcolo matematico, è elaborare una valutazione del rischio per ognuno di voi. In sostanza quantificare, se riesco, le varie scelte che avete e le loro rispettive conseguenze».

Riacquistando via via sicurezza, scrive sulla lavagna i numeri che descrivono le loro circostanze individuali e afferma: «Ora dovrò assegnare alcune variabili, in base a fattori come le vostre rispettive età, fedine penali, persone amate che vi aspettano fuori...»

Dopo alcune accese obiezioni da parte del capobanda, che Charlie ha indicato con la lettera «G» sulla lavagna, la lezione giunge al termine.

«Ecco qui. Fitchman, tu hai un punteggio di rischio di 14,9. 'W, il tuo è di 26,4, e 'G', hai un punteggio di rischio di... to', 7,9.»

Fitchman chiede che cosa significhi e Don risponde: «Vuol dire che Ben [«W» sulla lavagna] è quello che perderebbe di più andando in prigione».

Don e Charlie spiegano meglio questa conclusione, parlando della giovane età di Ben, del fatto che la sua fedina penale sia ancora pulita, dei suoi stretti legami famigliari e così via. In base a questi fattori, Charlie riassume la sua valutazione del rischio per il giovane uomo: «Dunque, come ho mostrato con i calcoli matematici, tu sei quello che ha più da perdere se non collabori».

Ciò che segue è indubbiamente il primo «patteggiamento indotto dalla matematica» nella storia della televisione! Inverosimile? Forse. Ma l'analisi matematica di Charlie era ineccepibile.

La valutazione del rischio come arma contro il terrorismo

Oggigiorno, la lotta contro il terrorismo si affida all'aiuto di vari strumenti matematici: il *data mining*, l'elaborazione dei segnali, l'analisi delle impronte digitali e vocali, la teoria della probabilità, la statistica e molti altri. Dal momento che sia le strategie dei terroristi sia quelle di difesa coinvolgono considerazioni su quello che farà la parte rivale, l'applicazione della teoria dei giochi è un'opzione attraente, proprio come lo è stata nel corso della guerra fredda. Ma come abbiamo visto nel caso del dilemma del prigioniero e del finto scenario rappresentato nell'episodio di *NUMB3RS*, l'uso della teoria dei giochi per determinare le linee d'azione migliori incontra alcuni limiti. Il ricorso a comunicazioni laterali e la creazione di accordi tra i giocatori, le incertezze su quali strategie stiano realmente utilizzando - quella che nel gergo della teoria dei giochi viene chiamata «incompletezza delle informazioni» - e la difficoltà di determinare quali profitti stiano effettivamente perseguendo, sono tutti fattori che insieme costituiscono una grossa sfida per gli studiosi di teoria dei giochi.

La valutazione dei rischi è un ingrediente fondamentale negli sforzi dei matematici di integrare o persino sostituire le analisi della teoria dei giochi. Un buon esempio è offerto in un articolo del 2002 di David L. Banks e Steven Anderson, dal titolo *Combining Game Theory and Risk Analysis in Counterterrorism: A Smallpox*

Example¹⁹

La loro analisi della minaccia di un attacco terroristico con il virus del vaiolo utilizza gli scenari su cui si sono concentrati molti esperti governativi e altri ricercatori. Essi comprendono tre categorie di possibili attacchi:

- nessun attacco;
- un unico attacco terroristico in una piccola area (come le famigerate «lettere all'antrace» circolate negli Stati Uniti dopo l'11 settembre);
- un attacco terroristico coordinato in più di una città;

e quattro scenari per la difesa;

- accumulare scorte di vaccino antivaiolo;
- accumulare scorte di vaccino e potenziare i sistemi di biosorveglianza;
- accumulare scorte di vaccino, potenziare i sistemi di biosorveglianza e vaccinare il personale a rischio;
- vaccinare tutti in anticipo (eccetto gli «immunocompromessi»).

Banks e Anderson considerano la matrice dei profitti, in base alla teoria dei giochi, per le tre strategie di attacco in combinazione con le quattro strategie di difesa, che dà come risultato dodici celle da riempire, ciascuna contenente il costo in dollari (o il suo equivalente) per la difesa. Per determinare i valori numerici da inserire in queste celle, i due autori propongono di compiere una valutazione del rischio separata per ciascuna cella. Ad esempio, la combinazione di strategie «nessun attacco», «accumulare scorte di vaccino» comporta un costo che essi descrivono (a partire dalle deliberazioni governative del giugno 2002) come:

$$ET_{Dry} + ET_{Avent} + ET_{Acamb} + VIG + PHIS,$$

dove

ET_{Dry} , ET_{Avent} = costi dei test di efficacia e sicurezza per i vaccini Dryvax e Aventis;

ET_{Acamb} = costo della produzione e sperimentazione del nuovo vaccino della Acambis;

VIG = costo delle dosi di immunoglobuline contro il virus *Vaccinici* per testare le reazioni avverse;

PHIS = costo derivante dalla predisposizione delle infrastrutture di sanità pubblica per gestire l'accumulo delle scorte.

Ai tempi dell'analisi degli autori, un contratto governativo fissava il costo per il nuovo vaccino della Acambis a 512 milioni di dollari, ma i costi per sperimentare i vaccini Dryvax e Aventis comprendono test clinici e possibili controlli ulteriori. Inoltre, c'è grande incertezza circa i costi della produzione e sperimentazione di dosi sufficienti di VIG e sui costi delle infrastrutture della sanità pubblica (PHIS). Per

¹⁹ In Alyson G. Wilson, Gregory D. Wilson e David H. Olwell (a cura di), *Statistical Methods in Counterterrorism*, Springer, New York, 2006.

l'analisi matematica degli autori la chiave consiste nel derivare stime di questi costi incerti dalle opinioni degli esperti. Anziché affidarsi soltanto all'ipotesi più verosimile per ogni costo, essi propongono di utilizzare intervalli di valori plausibili, espressi mediante distribuzioni di probabilità. Ad esempio, rappresentano il costo delle infrastrutture sanitarie pubbliche attraverso il familiare modello della curva a campana, con il centro in corrispondenza di 940 milioni di dollari e un'ampiezza (deviazione standard) di 100 milioni di dollari.

Una volta compiute le valutazioni dei rischi per le dodici possibili combinazioni di strategie attacco/difesa, Banks e Anderson vedono che cosa succede se si saggiano possibili matrici dei profitti - con un numero definito in ogni cella - ottenute utilizzando le distribuzioni di probabilità che rappresentano le opinioni degli esperti. E in sostanza come tirar fuori da un cappello le risposte possibili a tutte le domande senza risposta, generando una dopo l'altra diverse matrici dei profitti, ognuna delle quali potrebbe essere vera. Per ogni matrice, essi calcolano un punteggio che valuta la prestazione di ciascuna delle quattro strategie di difesa. Questi punteggi indicano i costi in cui incorre ogni strategia di difesa quando gli attaccanti utilizzano la loro strategia migliore (una «strategia maximin», nel gergo della teoria dei giochi).

Utilizzando le migliori opinioni degli esperti disponibili nel 2002, Banks e Anderson hanno scoperto nelle loro simulazioni al computer che la strategia più efficace per la difesa è quella di «vaccinare tutti». Ma si premurano di precisare che i loro risultati non sono definitivi; infatti i punteggi di tutte e quattro le strategie di difesa cadono in intervalli equivalenti, a indicare che l'incertezza nei dibattiti pubblici sulla strategia del governo statunitense non è del tutto infondata. Nel raccomandare l'applicazione dei loro metodi matematici alle future analisi delle minacce terroristiche e delle strategie difensive, Banks e Anderson affermano che è meglio usare i metodi della teoria dei giochi e della valutazione del rischio *insieme* piuttosto che separatamente. Questo perché da un lato la valutazione del rischio da sola non riesce a cogliere il tipo di interazione tra gli avversari («se lui fa questo, io posso fare quello») che la teoria dei giochi invece incorpora per sua natura, mentre dall'altro la teoria dei giochi normalmente richiede profitti definiti piuttosto che l'analisi probabilistica dei profitti consentita dalla valutazione del rischio.

La ricerca operativa sul contrabbando di armi nucleari

Tra le minacce terroristiche che furono al centro di grandi dibattiti negli Stati Uniti durante le campagne per le elezioni presidenziali del 2004 vi era la possibilità che materiali e armi nucleari venissero portati di contrabbando nel Paese tramite i porti marittimi. Molti credono che un sistema di difesa contro questa minaccia debba coinvolgere ispezioni dei container navali nei porti esteri prima che vengano caricati sulle navi dirette negli Stati Uniti. Nel secondo porto più trafficato del mondo, a Hong Kong, l'associazione degli operatori del Container Terminal ha messo a punto un progetto dimostrativo per tali ispezioni, che prevede le seguenti procedure:

- gli autocarri che trasportano un container da caricare su una nave devono passare attraverso un cancello;
- settantacinque metri prima del cancello gli autocarri devono passare attraverso un portale ed essere esaminati da un rilevatore di radiazioni RPM (*radiation portal monitor*) che individua le emissioni di neutroni;
- se il dispositivo RPM non è in grado di stabilire che il contenuto del container è assolutamente sicuro, il container può essere indirizzato a un ufficio di controllo doganale per un tipo diverso di ispezione e per un possibile esame fisico del suo contenuto.

Il programma pilota di Hong Kong prevedeva che gli autocarri attraversassero il portale con il rilevatore RPM a una velocità di 16 chilometri orari, in modo da permettere una durata del test di circa tre secondi. Test più lunghi consentirebbero la rilevazione di tassi più bassi di emissione neutronica, ma rallentare l'avanzamento della fila comporterebbe dei costi. Il protocollo di ispezione deve specificare anche altre variabili, tra cui l'individuazione dei container che dovranno essere sottoposti a controlli più approfonditi in base al sistema automatizzato ATS (*Automated Targeting System*) del servizio doganale degli Stati Uniti. Questo è un sistema specializzato che utilizza i dati associati all'imbarco di ciascun container, ovvero il suo manifesto di carico, unitamente a possibili informazioni di intelligence e a indicatori osservabili che suggeriscono la probabilità che un container sia «sporco».

La principale preoccupazione del progetto dimostrativo di Hong Kong è evitare di rallentare il flusso di autocarri nell'area di scarico. Le analisi con il dispositivo RPM devono essere condotte senza provocare un rallentamento, giacché questo aumenterebbe significativamente il costo delle operazioni portuali. Uno dei dettagli del programma prevede che gli autocarri, dopo aver attraversato il cancello, si dispongano in quattro file, ognuna gestita da un sorvegliante che controlla l'identità dei conducenti e dice loro dove andare a scaricare il container.

Il sistema di Hong Kong è stato progettato in modo da essere altamente efficiente. Ma proprio come Charlie Eppes è raramente soddisfatto di un sistema che non ha avuto l'opportunità di analizzare con strumenti matematici, allo stesso modo un gruppo di studiosi impegnati in quelle che vengono oggi chiamate «ricerche operative» (si veda più avanti la spiegazione di questo termine) hanno deciso di mettere a punto un modello matematico per analizzare tutti gli aspetti del sistema di Hong Kong: l'esame con il rilevatore RPM della fila di autocarri prima del cancello principale, il protocollo seguito per analizzare i risultati del test e selezionare alcuni container per ulteriori controlli, e il costo dell'intera operazione.

Nel loro articolo *The Optimal Spatial Deployment of Radiation Portal Monitors Can Improve Nuclear Detection at Overseas Ports* (2005), Lawrence M. Wein, Yifan Liu, Zheng Cao e Stephen E. Flynn analizzano da un punto di vista matematico un insieme di progetti alternativi per l'ispezione dei container navali al fine di stabilire se è possibile migliorare l'efficacia del progetto di Hong Kong. Prima di spiegare le loro idee dovremmo però rispondere alla seguente domanda: che cos'è la ricerca operativa e in che modo potrebbe portare a un miglioramento nella progettazione del

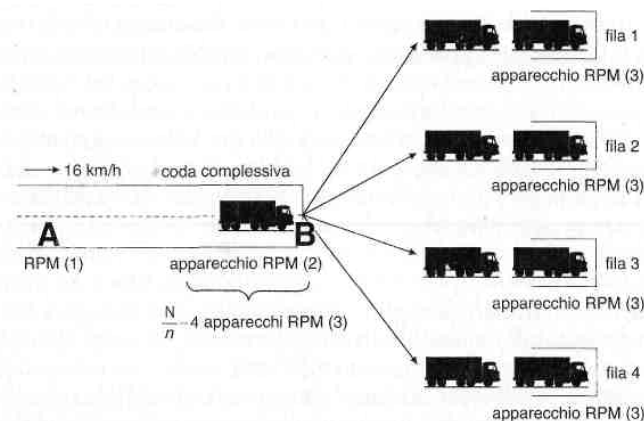
sistema?

Il termine «ricerca operativa» (*Operations Research* od OR) fa riferimento a un'ampia gamma di strumenti e metodi matematici applicati in quella che viene ogni tanto chiamata «la scienza del meglio», ovvero l'analisi di come si svolgono le operazioni condotte nel mondo reale e di come si potrebbe intervenire per farle funzionare meglio. Originariamente applicata nel periodo successivo alla Seconda guerra mondiale a sistemi militari come la logistica, il rifornimento e le manovre tattiche navali, la OR ha presto trovato altri impieghi negli studi per accrescere l'efficienza delle operazioni affaristiche, delle strutture pubbliche (quali aeroporti, parchi di divertimento e ospedali), dei servizi pubblici (come dipartimenti di polizia e personale paramedico) e di molti uffici e servizi governativi. Gli strumenti utilizzati nella ricerca operativa sono tutti strumenti matematici quali, ad esempio, modelli per studiare il comportamento dei sistemi complessi, algoritmi, simulazioni al computer, teoria della probabilità e analisi statistica. Talvolta il termine «scienza gestionale» viene utilizzato più o meno come sinonimo di ricerca operativa.

Tra le applicazioni della OR nelle operazioni di polizia si annoverano indagini matematiche su come distribuire le pattuglie nelle zone ad alto indice di criminalità, su come sorvegliare i bersagli più a rischio di attacco e su come organizzare e analizzare i dati da utilizzare nelle indagini. In molte università esistono dipartimenti di ricerca operativa o scienza gestionale e i docenti solitamente, oltre a insegnare, compiono sia ricerca teorica sui metodi matematici sia consulenza sui problemi reali.

Una delle componenti classiche della OR è la teoria delle code (*Queueing Theory*), una branca della teoria della probabilità che indaga i fenomeni associati alle «file di attesa», e cerca di fornire risposte a domande come «qual è il modo più efficiente di organizzare una fila di attesa in una banca?» oppure «quanti sportellisti occorrono per limitare il tempo medio di attesa a cinque minuti se i clienti arrivano a un dato ritmo r e ognuno richiede un tempo medio di t minuti per essere servito?»

Torniamo ora agli autocarri nel porto di Hong Kong che aspettano pazientemente di scaricare i container sulle navi. Vedremo in che modo la ricerca operativa, come quella condotta da Wein, Liu, Cao e Flynn, impiega l'analisi matematica per progettare sistemi migliori e per calcolarne la resa e i costi. Iniziamo con una figura che rappresenta il flusso di autocarri e container attraverso il cancello principale:



L'esperimento dimostrativo di Hong Kong colloca un apparecchio RPM nel punto A, a 75 metri dal punto B, in cui è situato il cancello principale. Questo assicura che

gli autocarri possano passare davanti al monitor a una velocità regolare di 16 chilometri orari. Dal momento che ogni container navale di 14 metri è posto sull'autocarro nel senso della lunghezza, esso impiega circa tre secondi ad attraversare il portale, così che il monitor può conteggiare i neutroni emessi per tre secondi. Il numero di neutroni conteggiato dipende dai valori di cinque fattori:

A = area del rilevatore di neutroni = 0,3 metri quadrati

ϵ = efficienza del rilevatore = 0,14

S = quantità di neutroni emessi al secondo (dipendente dalla sorgente)

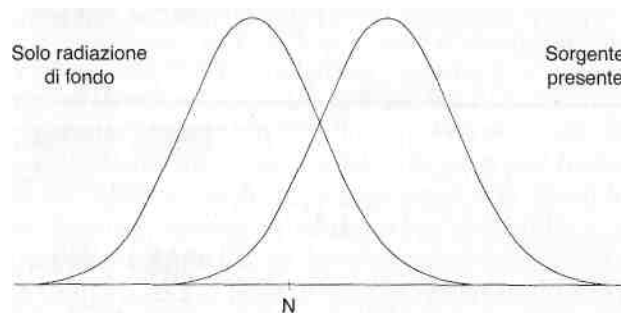
τ = durata del test = numero di secondi per cui l'apparecchio RPM può contare i neutroni

r = distanza dell'apparecchio RPM dal centro del container = 2 metri

Il risultato è:

$$\text{numero medio di neutroni conteggiati} = A\epsilon S\tau / 4\pi r^2$$

La variabilità del numero conteggiato è descritta da una curva a campana la cui ampiezza (deviazione standard) è pari a circa 2,8 volte la radice quadrata della media. Poiché esiste una radiazione neutronica di fondo a un tasso B , inferiore a S , anch'essa può essere rappresentata con una curva a campana, il che porta a un'immagine come questa:



Il valore di soglia N è il numero di neutroni rilevati che richiede un ulteriore livello di controllo: domandare a un analista umano di esaminare la scansione prodotta da un sistema a raggi gamma VACIS, progettato per individuare la presenza nei container di eventuali materiali densi utilizzati per schermare le emissioni. Se la persona che esamina la scansione non è in grado di confermare la sicurezza del container, l'autocarro viene condotto in un altro luogo dove gli ispettori doganali eseguiranno una scansione con raggi X ad alta energia e, se necessario, apriranno il container per ispezionare il suo contenuto manualmente. Questi controlli rappresentano una parte piuttosto costosa del sistema complessivo, ma sono in grado di individuare in maniera affidabile la presenza di materiale radioattivo. Anche se nessun container supera la soglia del test RPM, ci si può aspettare che un 5 per cento sia segnalato per l'ispezione VACIS in quanto giudicato sospetto dal sistema automatizzato ACS, che impiega un'analisi separata della sicurezza dei container basata sulle informazioni circa la loro provenienza.

Altre variabili chiave sono le probabilità di successo delle analisi VACIS e a raggi X e i costi comprendono:

- 250 dollari per ciascuna scansione con raggi X ad alta energia;
- 1500 dollari per ciascuna apertura e ispezione manuale di un container;
- 100.000 dollari per il costo annuo di ciascun dispositivo RPM.

L'obiettivo dell'intera analisi è di mettere a punto sistemi che per un dato costo annuo raggiungano il valore più basso possibile del limite di rilevazione:

S_D = livello di emissione di neutroni al secondo dalla sorgente radioattiva che il dispositivo RPM è in grado di rilevare

con il requisito che la probabilità che l'apparecchio RPM rilevi quel livello di emissione sia almeno del 95 per cento. Anche la possibilità di risultati falsi positivi - cioè container che producono un conteggio al livello N o superiore a causa della naturale radiazione di fondo - è considerata nel modello, in quanto i controlli ulteriori che si renderebbero necessari in questi casi implicano altri costi.

Una volta considerate tutte le variabili in gioco - entro un limite sul costo annuo e tenendo presente la necessità di non rallentare il flusso degli autocarri - che cosa si può fare da un punto di vista matematico per migliorare il sistema? Wein e gli altri coautori dell'articolo analizzano il progetto esistente insieme a tre modalità alternative, potenzialmente migliori:

- Progetto 1 (esistente) = un apparecchio RPM collocato 75 metri prima del cancello principale.
- Progetto 2 = un apparecchio RPM collocato in corrispondenza del cancello principale.
- Progetto 3 = 4 apparecchi RPM collocati dopo il cancello, uno per ogni fila di autocarri.
- Progetto 4 = aggiungere al progetto 3 una serie di 10 apparecchi RPM nella fila di fronte al cancello B.

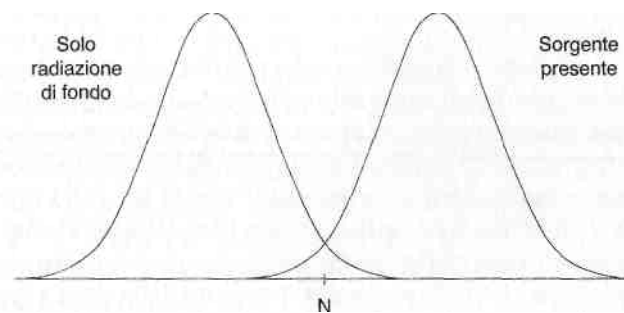
In base ai presupposti quantitativi del loro articolo, gli autori mostrano che in un dato intervallo di valori per il costo annuo:

- Il progetto 2 migliora il limite di rilevazione S_D di 2 volte a parità di costo.
- Il progetto 3 migliora S_D di altre 4 volte.
- Il progetto 4 migliora ulteriormente S_D di 1,6 volte.

Pertanto, il miglioramento complessivo implicato nel passaggio dal progetto 1, utilizzato nell'esperimento di Hong Kong, al progetto 4 è una riduzione di 13 volte del livello di emissione neutronica dalla sorgente radioattiva che il sistema è in grado di rilevare. Come si ottiene questo risultato?

La risposta è articolata in due parti. La prima consiste nel fatto che più lunga è la durata del test, τ , maggiore è la probabilità che si riesca a individuare correttamente la presenza di un'emissione neutronica aggiuntiva, oltre a quella di fondo. Per la stessa ragione per cui gli statistici raccomandano sempre di esaminare, se possibile, un campione più grande di dati, un tempo più lungo a disposizione degli apparecchi

RPM per effettuare il conteggio dei neutroni ha l'effetto di allontanare le due curve a campana in modo da ottenere un'immagine come questa:



Dato che ora le due curve sono molto meno sovrapposte, il valore di soglia N usato per la rilevazione può essere portato a un livello relativamente inferiore senza che ciò aumenti la frequenza di falsi positivi. In alternativa, si può fissare il livello di N in modo che i risultati falsi positivi si presentino con la stessa frequenza di prima e che le rilevazioni corrette si verifichino quando il valore di S (l'emissione di neutroni al secondo dipendente dalla sorgente) è più basso. In tal modo il limite di rilevazione S_D viene ridotto.

La seconda parte della risposta offerta dagli autori proviene dall'analisi dei modelli, elaborati in base alla teoria delle code, per i quattro progetti. Lo scopo è di esporre i container a tempi più lunghi di analisi, cioè di accrescere il valore di τ . La possibilità di miglioramento è chiara, dal momento che l'apparecchio RPM nel punto A ha soltanto tre secondi per esaminare ogni autocarro, mentre gli autocarri attendono molto più a lungo per passare attraverso il processo di ispezione.

Trasferendo il dispositivo RPM dal punto A al punto B, il progetto 2 trae vantaggio dal fatto che talvolta nella fila fluiscono più autocarri del solito e gli autocarri devono quindi stare fermi in coda per un po' dietro il cancello. Pertanto, se l'apparecchio RPM viene collocato in quel punto, esso potrà esaminare gli autocarri in attesa per un tempo più lungo.

Sostituendo il singolo apparecchio RPM nel punto B con quattro apparecchi, uno per ogni fila, il progetto 3 porta a un miglioramento ancor più significativo rispetto al progetto 1, dal momento che il tempo medio necessario perché gli ispettori doganali facciano passare gli autocarri in testa alle file è di sessanta secondi. Collocando una serie di altri apparecchi RPM prima del cancello principale, B, il progetto 4 consente un ulteriore aumento della durata del test e, conseguentemente, un'ulteriore riduzione del limite di rilevazione.

Ma come risolvere il problema dei costi di tutti questi apparecchi RPM aggiuntivi? Entro qualunque budget annuale prefissato, questi costi possono essere compensati dalla diminuzione della frequenza degli esiti falsi positivi a ogni stadio del processo di controllo, la quale riduce i costi delle scansioni a raggi X e delle ispezioni manuali. L'obiettivo principale del tipo OR di modellizzazione e ottimizzazione matematica (una parola che in gergo matematico significa «trovare il modo migliore») proposto dalla ricerca operativa è di stabilire quali variabili di un sistema debbano essere corrette per migliorarne la prestazione complessiva, mantenendo però un vincolo su altre variabili come, in questo caso, il costo totale dell'operazione e la velocità del

flusso di autocarri. Se sapesse del lavoro dei matematici impegnati nella ricerca operativa, come Wein, Liu, Cao e Flynn, Charlie Eppes ne sarebbe fiero.

Controllare i passeggeri delle linee aeree

A partire dai tragici eventi dell'11 settembre 2001 il governo statunitense ha investito ingenti risorse finanziarie e umane per prevenire il ripetersi di attacchi dello stesso tipo. Quell'episodio intensificò gli sforzi del governo di accrescere la sicurezza delle linee aeree attraverso un sistema già in uso dal 1998. Chiamato CAPPS (da *Computer Assisted Passenger Prescreening System*), tale sistema poggia su alcune informazioni di base che una compagnia aerea ottiene nel momento in cui un passeggero acquista un biglietto: nome, indirizzo, modalità di pagamento e così via. La compagnia aerea utilizza quelle informazioni per verificare la presenza del nome del passeggero nella «lista di interdizione al volo» della Transportation Security Administration, una lista nera di individui segnalati come terroristi noti o sospetti, e per calcolare un «punteggio di rischio» in base ai profili dei terroristi. Questi profili sono elenchi di caratteristiche tipiche dei terroristi, ricavati dall'analisi statistica dei dati raccolti per molti anni sulle abitudini di volo di terroristi noti. Se il nome del passeggero figura nella lista nera, o se il punteggio di rischio basato sui profili è abbastanza alto, la compagnia aerea sottopone il passeggero e il suo bagaglio a controlli «di secondo livello», più intensivi di quelli normalmente effettuati.

Un sistema simile era stato istituito dopo una lunga serie di dirottamenti di aerei di linea (più di cinquanta) avvenuti negli anni 1968 e 1969; questi eventi avevano portato alla creazione di un «profilo del dirottatore» che fu utilizzato per molti anni e poi abbandonato. Sebbene i dettagli specifici sia del profilo del dirottatore sia del profilo del terrorista siano strettamente riservati, alcune delle loro caratteristiche sono state spesso ipotizzate nei dibattiti pubblici. (Ad esempio, un uomo giovane che viaggia da solo farebbe meglio a non acquistare un biglietto di sola andata, in particolare se paga in contanti.)

Dopo l'11 settembre la neonata Transportation Security Administration si è assunta la responsabilità non solo di elaborare una «lista di interdizione al volo» ma anche di compiere le analisi statistiche necessarie per migliorare l'efficacia dei profili di terroristi. Gli esperti esterni agli ambienti governativi ritengono che per affinare i profili dei terroristi la TSA faccia uso di reti neurali (si veda il capitolo 3). E senza dubbio ragionevole che le autorità federali cerchino di isolare dalla popolazione generica quei passeggeri dei viaggi aerei che potrebbero essere considerati ad alto rischio come potenziali terroristi, per poi sottoporli a controlli e a indagini ulteriori. Questa è la logica del sistema CAPPS. Ma quanto ci si può aspettare che funzioni un sistema del genere? La risposta, come vedremo, non è semplice come potrebbe apparire a prima vista.

Due studenti del MIT analizzano il sistema CAPPS

Nel maggio del 2002, due studenti del MIT fecero notizia annunciando un articolo che avevano preparato per una lezione sul tema *Etica e legge nella frontiera elettronica*. Samidh Chakrabarti e Aaron Strauss pensarono che l'analisi del CAPPS sarebbe stato un argomento interessante per la lezione, e i risultati della loro analisi matematica furono così sorprendenti che il professore li incitò a diffonderli su scala più vasta, cosa che i due studenti fecero pubblicando il loro studio in Internet. L'articolo, intitolato *Carnival Booth: An Algorithm for Defeating the Computer-Assisted Passenger Screening System*, fece scalpore perché dimostrava, con chiara analisi logica e matematica, come i terroristi potrebbero adattare con relativa facilità il loro comportamento in modo da rendere il CAPPS meno efficace di un sistema puramente casuale di selezione dei passeggeri sospetti. I presupposti dell'analisi di Chakrabarti e Strauss sono i seguenti:

- indipendentemente da quale sistema venga usato per selezionare le persone sospette, solo l'8 per cento dei passeggeri può essere sottoposto a controlli di secondo livello;
- nel CAPPS, il requisito federale di selezionare a caso un « x per cento dei passeggeri» per ulteriori controlli è soddisfatto selezionando a caso il 2 per cento dei passeggeri;
- fra i terroristi destinati a controlli secondari, tre su quattro saranno intercettati con successo;
- senza questi controlli secondari, solo un terrorista su quattro sarà intercettato con successo;
- la percentuale p di terroristi che non sono destinati a controlli secondari dal sistema di selezione casuale ma che vengono segnalati dal CAPPS è sconosciuta.

Le assunzioni sulle percentuali effettuate da Chakrabarti e Strauss non sono casuali. Piuttosto, essi basano la loro analisi sulle migliori stime pubblicamente disponibili delle percentuali effettive, che sono dati segreti del governo. I loro risultati non dipendono sostanzialmente dai valori esatti di quelle percentuali. La percentuale sconosciuta p dipende da quanto deve essere alto il punteggio di rischio per giudicare un passeggero sospetto. Per soddisfare il requisito in base al quale «non più dell'8 per cento» dei passeggeri può essere sottoposto a controlli ulteriori, la soglia per il punteggio di rischio deve essere scelta in modo che sia raggiunta dal 6 per cento dei passeggeri che sfuggono alla selezione casuale.

Quindi, la percentuale complessiva di terroristi che saranno intercettati impiegando il sistema CAPPS è:

$$(*) \frac{3}{4} \text{ di } p \% + \frac{3}{4} \text{ di } 2\% + \frac{1}{4} \text{ della percentuale restante}$$

Per effettuare il confronto, Chakrabarti e Strauss considerano un sistema

«puramente casuale», in cui l'8 per cento dei passeggeri che può essere sottoposto a controlli secondari viene selezionato a caso dalla lista di tutti i passeggeri. In tal caso la percentuale complessiva di terroristi intercettati sarà:

$$(**) \frac{3}{4} \text{ di } 8\% + \frac{1}{4} \text{ di } 92\% = 6\% + 23\% = 29\%$$

Confrontando (*) e (**), la domanda ovvia è: «Quale metodo intercetta una percentuale di terroristi più alta?» La risposta dipende dal valore di p , la percentuale sconosciuta di terroristi che vengono selezionati perché corrispondono al profilo. Vediamo alcuni esempi:

Valore di p	Percentuale complessiva di terroristi intercettati
2%	27%
4%	28%
6%	29%
8%	30%
10%	31%

Da questi esempi è chiaro che l'efficacia dei due sistemi, il CAPPS e quello di selezione casuale, è la stessa quando la percentuale p di terroristi che vengono sottoposti a controlli secondari perché corrispondono al profilo è uguale a 6.

Arriviamo quindi al cuore della questione. Si potrebbe dire: «Sicuramente possiamo aspettarci che la percentuale dei terroristi che corrispondono al profilo sia più alta di un irrisorio 6 per cento!» E qui che entra in gioco il fenomeno che Chakrabarti e Strauss chiamano «effetto luna park». Essi affermano che, siccome il profilo del terrorista è stabile, e poiché le cellule terroristiche comprendono membri con una varietà di caratteristiche, una cellula che vuole che uno dei suoi membri salga su un aereo per compiere un attacco può utilizzare la seguente strategia:

- sondare il sistema CAPPS con qualche «giro di prova», vale a dire facendo acquistare biglietti aerei da alcuni dei suoi membri per vedere quali vengono segnalati in base al profilo e quali no;
- per la vera missione di attacco, utilizzare i membri che non sono stati segnalati nei giri di prova e che hanno pertanto probabilità molto basse di essere segnalati in base allo stesso profilo.

Chakrabarti e Strauss chiamano questa tattica effetto luna park perché ricorda gli imbonitori al luna park che gridano: «Fatevi avanti, provate a vincere!» Gli aspiranti attentatori che costituiscono una minaccia reale sono i «vincitori» che non vengono segnalati per ulteriori controlli quando «si fanno avanti» sfidando il sistema CAPPS. Come i due autori del MIT spiegano per esteso, l'applicabilità di tale strategia dipende soltanto da due fattori fondamentali. Innanzitutto, il profilo del CAPPS resta uguale nel tempo - almeno per brevi periodi - il che comporta che se un individuo non viene segnalato una volta passerà inosservato anche la volta successiva. In

secondo luogo, delle cellule terroristiche fanno parte membri con una notevole varietà di caratteristiche, il che rende probabile che almeno uno di loro possa superare l'esame del profilo. A sostegno di quest'ultimo punto, gli autori descrivono alcuni noti terroristi coinvolti in episodi recenti, come il «talebano americano» John Walker Lindh, un diciannovenne della Contea di Marin, e Richard Reid, il cittadino britannico con madre inglese e padre giamaicano per colpa del quale oggi tutti noi dobbiamo toglierci le scarpe prima di salire su un aereo.

I due ricercatori del MIT inclusero nel loro articolo alcune analisi più sofisticate basate su simulazioni al computer che incorporavano un certo grado di variabilità e di incertezza nei punteggi di rischio calcolati dal CAPPs per ogni singolo terrorista. Ad esempio, essi scoprirono che, per qualche terrorista, le prove ripetute renderebbero la sua probabilità di essere segnalato inferiore a quella di un passeggero qualunque. In tal caso, la probabilità del CAPPs di intercettare un vero attacco perpetrato da uno di questi terroristi sarebbe inferiore a quella di un sistema di selezione puramente casuale.

Il potere della matematica è tale che persino due brillanti studenti universitari, scrivendo un articolo per un esame, possono offrire un contributo significativo a una questione così importante come la sicurezza delle linee aeree.

LA MATEMATICA IN TRIBUNALE

Bene, quindi Charlie ha tirato fuori tutte le sue risorse matematiche e ancora una volta Don, grazie a lui, è riuscito a incastrare il sospetto. E così che generalmente si conclude un episodio di *NUMB3RS*, ma nella vita reale spesso l'uso della matematica non finisce qui. La matematica viene impiegata non solo per smascherare i criminali, ma anche durante i processi in tribunale.

Un esempio è dato dall'uso di fotografie migliorate attraverso strumenti matematici, come nel caso del pestaggio di Reginald Denny descritto nel capitolo 5; un altro sono i calcoli delle probabilità che devono accompagnare la presentazione di prove del DNA, come abbiamo visto nel capitolo 7. Ma ci sono molte altre occasioni in cui gli avvocati, i giudici e le giurie devono soppesare prove matematiche. Come dimostra il primo caso trattato in questo capitolo, se sbagliano a valutare queste prove, il risultato può essere un drammatico errore giudiziario.

La bionda con la coda di cavallo

Il 18 giugno 1964, poco prima di mezzogiorno, nell'area di San Pedro a Los Angeles, una donna anziana di nome Juanita Brooks stava tornando a casa dopo aver fatto alcune compere in drogheria. Usando un bastone, stava trasportando la spesa in un cestino di vimini, sopra cui aveva appoggiato la borsa. Dopo aver imboccato un vialetto, si fermò a raccogliere una scatola di cartone vuota e improvvisamente si sentì spingere a terra. Seppure stordita dalla caduta, riuscì a guardare in alto e vide una giovane donna con i capelli biondi raccolti in una coda di cavallo che correva lungo il vialetto con la sua borsa. Vicino allo sbocco del vialetto, un uomo di nome John Bass stava annaffiando il prato di fronte alla sua casa quando sentì gridare. Si voltò verso il vialetto e ne vide uscire di corsa una donna che entrò in un'automobile gialla dall'altra parte della strada. L'auto si mise in moto, fece inversione e partì, passandogli a due metri di distanza. Secondo le descrizioni che Bass fornì in seguito, il guidatore era un maschio «negro» (era il 1964) con la barba e i baffi, mentre la donna era bianca, alta più di un metro e settanta e con i capelli biondi raccolti in una coda di cavallo.

Juanita Brooks denunciò il furto alla polizia di Los Angeles, dicendo che la borsa rubata conteneva tra 35 e 40 dollari. Molti giorni dopo, la polizia arrestò Janet Louise Collins e suo marito Malcolm Ricardo Collins, che alla fine furono accusati del crimine e processati davanti a una giuria.

L'avvocato dell'accusa si trovò di fronte a un'interessante sfida. Nessuno dei due testimoni oculari, Juanita Brooks e John Bass, fu in grado di identificare gli imputati.

(In precedenza Bass non era riuscito a identificare Malcolm Collins in un confronto all'americana, nel quale il sospetto era apparso senza la barba che aveva ammesso di aver portato in passato, ma non il giorno del furto, a suo dire.) Vi era un po' di confusione dovuta al fatto che i testimoni avevano dichiarato che la donna indossava abiti «scuri», mentre altre persone interrogate dalla polizia avevano visto Janet Collins poco prima del furto con addosso abiti chiari. In che modo l'avvocato dell'accusa poteva dimostrare davanti alla giuria che i due imputati erano colpevoli del furto della borsa?

La soluzione per cui optò fu di adottare un nuovo approccio. Decise di chiamare a testimoniare un esperto: un docente di matematica di un'università statale. La testimonianza dell'esperto riguardava le probabilità e come combinarle. Nello specifico, al matematico fu chiesto di spiegare la regola del prodotto per determinare la probabilità che più eventi si presentino insieme sulla base delle probabilità associate al verificarsi di ogni singolo evento.

L'avvocato chiese al matematico di considerare sei caratteristiche riguardanti i due perpetratori del furto:

- uomo di colore con la barba;
- uomo con i baffi;
- donna bianca con i capelli biondi;
- donna con la coda di cavallo;
- coppia mista in un'automobile;
- automobile gialla.

Dopo di che fornì al matematico alcuni numeri indicanti le ipotetiche probabilità che una coppia (innocente) qualunque potesse soddisfare tutti questi elementi descrittivi. Ad esempio, chiese al matematico di assumere che solo in una coppia su dieci il partner maschile fosse un «uomo di colore con la barba», e che gli uomini con i baffi (nel 1964) fossero uno su quattro. Domandò poi all'esperto di spiegare come calcolare la probabilità che il partner maschile di una coppia possedesse *entrambe* le caratteristiche: «uomo di colore con la barba» e «uomo con i baffi». L'esperto descrisse una procedura ben nota ai matematici, chiamata «regola del prodotto per gli eventi indipendenti». Essa afferma che «se due eventi sono indipendenti, la probabilità che si presentino insieme è il prodotto delle loro probabilità individuali».

Dunque, nel caso ipotetico proposto dall'avvocato dell'accusa, se gli eventi fossero effettivamente indipendenti (vedremo più avanti che cosa significa esattamente), allora si potrebbe usare la regola del prodotto per calcolare la probabilità che un individuo sia un uomo di colore con la barba e i baffi, moltiplicando le due probabilità date:

$$\begin{aligned} &P(\text{uomo di colore con la barba e i baffi}) \\ &= P(\text{uomo di colore con la barba}) \times P(\text{uomo con i baffi}) \\ &= 1/10 \times 1/4 = 1/(10 \times 4) = 1/40 \end{aligned}$$

La lista completa delle probabilità che l'avvocato dell'accusa chiese al matematico

di assumere come dati di partenza era:

- uomo di colore con la barba: 1 su 10;
- uomo con i baffi: 1 su 4;
- donna bianca con i capelli biondi: 1 su 3;
- donna con la coda di cavallo: 1 su 10;
- coppia mista in un'automobile: 1 su 1000;
- automobile gialla: 1 su 10.

L'avvocato dell'accusa chiese al matematico di considerare questi numeri come stime prudenti, a significare che le probabilità effettive erano almeno così piccole, ma potevano essere anche più basse. A quel punto il matematico procedette con la spiegazione di come fare a combinare queste probabilità in modo da calcolare la probabilità complessiva che una coppia qualunque rispondesse a tutte le sopraccitate descrizioni. Partendo dal presupposto che gli eventi fossero indipendenti, il matematico affermò nella propria deposizione che il calcolo corretto della probabilità complessiva, chiamiamola *PC*, utilizzava la stessa regola del prodotto, e cioè che per ottenere la probabilità che una coppia presa a caso rispondesse a tutti i requisiti elencati occorreva moltiplicare tra loro le probabilità individuali associate a ogni singola caratteristica. Facendo questo, il risultato che si ottiene è:

$$\begin{aligned} PC &= 1/10 \times 1/4 \times 1/3 \times 1/10 \times 1/1000 \times 1/10 \\ &= 1/(10 \times 4 \times 3 \times 10 \times 1000 \times 10) \\ &= 1/12.000.000 \end{aligned}$$

Uno su dodici milioni!

Quando l'avvocato dell'accusa fornì all'esperto le varie probabilità - 1/10, 1/4 ecc. - che avrebbe dovuto usare per calcolare la probabilità complessiva, specificò che quei numeri particolari avevano soltanto un valore «illustrativo». Ma nel suo discorso finale sostenne che erano «stime prudenti» e che pertanto «la probabilità che un'altra coppia di persone, diversa dai due imputati, si trovasse lì, [...] che presentasse tutte le somiglianze [...], è circa uno su un miliardo».

La giuria dichiarò Malcolm e Janet Collins colpevoli del reato di cui erano stati accusati. Ma fu giusta quella sentenza? Erano corretti i calcoli del matematico? E vero che, come sostenne l'avvocato dell'accusa, c'era solo «una possibilità su un miliardo» che i due imputati fossero innocenti? Oppure la corte si trovò semplicemente coinvolta in una clamorosa farsa giudiziaria? Malcolm Collins era di questo avviso e si appellò contro la sentenza.

Nel 1968 la corte suprema dello Stato della California annunciò la propria decisione sul caso *People v. Collins*, 68 Cal.2d319, e il suo parere scritto è diventato un classico nello studio delle prove giudiziarie. Generazioni di studenti di legge hanno studiato il caso come un esempio di uso della matematica in tribunale.

Ecco che cosa affermava il parere dei giudici (approvato con sei voti favorevoli e uno contrario):

Ci troviamo di fronte a un nuovo problema: se la prova costituita dalla probabilità matematica sia stata adeguatamente introdotta e utilizzata dall'accusa in un caso penale [...] Quando, nella ricerca della verità, le persone incaricate di accertare i fatti si affidano all'aiuto della matematica, vera e propria strega ammaliatrice nella nostra società computerizzata, devono fare attenzione a non cadere vittima dei suoi incantesimi. Concludiamo che nel verbale che abbiamo esaminato l'imputato non avrebbe dovuto essere dichiarato colpevole sulla base delle probabilità e che pertanto egli ha diritto a un nuovo processo. Annulliamo la sentenza [...]

Il parere espresso dalla maggioranza nel caso Collins è un esempio affascinante dell'interazione tra due discipline accademiche: la giurisprudenza e la matematica. A dire il vero, i giudici si preoccuparono di precisare che non trovavano «alcuna incompatibilità intrinseca tra le [due] discipline» e che non intendevano in nessun modo «abbassare» la matematica al ruolo di «strumento ausiliario nella procedura di accertamento dei fatti» svolta dalla legge. Nondimeno, la corte dichiarò di non poter approvare il modo in cui la matematica era stata impiegata nel caso Collins.

La sua completa demolizione del ricorso alla matematica compiuto dall'accusa in quel caso giudiziario comprendeva tre elementi principali:

- la contrapposizione tra uso adeguato della «matematica come prova» e uso inadeguato («matematica come magia»);
- l'insuccesso nel dimostrare che l'argomentazione matematica addotta si applicava effettivamente al caso in questione;
- la grande fallacia logica che si annidava nell'affermazione dell'accusa secondo cui vi era solo «una possibilità su un miliardo» che gli imputati fossero innocenti.

Vediamo esattamente che cosa non funzionava nel ragionamento dell'avvocato dell'accusa.

Matematica: evidenza delle prove o magia?

La legge riconosce due modi principali in cui la testimonianza di un esperto può fornire una prova ammissibile. Un esperto può testimoniare in base alle proprie conoscenze circa fatti pertinenti, oppure può rispondere a ipotetiche domande su dati validi che sono già stati presentati come prove. Quindi, ad esempio, un esperto potrebbe fornire una testimonianza sulla percentuale - poniamo, a Los Angeles - di automobili gialle, o di donne bionde, ammesso che esistano dati statistici a sostegno delle sue dichiarazioni. E un matematico potrebbe rispondere a ipotetiche domande quali «come combinerebbe queste probabilità in modo da determinare una probabilità complessiva?», ammesso che esse si fondino su dati validi. Nel caso Collins, però, la corte suprema trovò che l'avvocato dell'accusa «non aveva fatto alcun tentativo di offrire simili prove» della validità dei dati di partenza. Inoltre, la corte fece notare che

il ragionamento matematico dell'accusa poggiava sull'assunto che le descrizioni fornite dai testimoni oculari fossero al cento per cento corrette in tutti i dettagli e che nessun travestimento (come una barba finta) fosse stato usato dai veri autori del crimine. (Il verbale del processo registrava testimonianze discordanti sul colore degli abiti indossati dalla donna, e sul fatto che l'uomo avesse o meno la barba.)

La corte puntualizzò che è tradizionalmente compito della giuria valutare l'attendibilità delle descrizioni fornite dai testimoni, la possibilità che siano stati usati travestimenti, e cose simili. Ma queste non sono considerazioni cui è possibile assegnare probabilità numeriche. Inoltre, la corte suprema riteneva che il fascino della «conclusione matematica» dell'uno su dodici milioni fosse probabilmente troppo irresistibile nella sua apparente «accuratezza scientifica» perché venisse svalutata come avrebbe dovuto nella normale valutazione dell'attendibilità delle prove. La corte scrisse: «Di fronte a un'equazione che ha la pretesa di fornire un indice numerico per la probabilità di colpevolezza, poche giurie potrebbero resistere alla tentazione di attribuire a quell'indice un peso spropositato». Questo è al cuore della «magia» che a parere della corte suprema aveva ammaliato i giurati nel caso Collins.

Era corretta la conclusione matematica?

Tralasciando la questione dell'ammissibilità di un ricorso alla matematica come quello consentito dalla corte originaria, vediamo se il ragionamento matematico di per sé era corretto. Anche ammettendo che i numeri scelti dall'avvocato dell'accusa per le probabilità di ogni singola caratteristica - uomo di colore con la barba e così via - si basassero su prove effettive e fossero accurati al cento per cento, il calcolo che egli chiese al matematico di effettuare dipende da un presupposto cruciale: che nella popolazione generale tali caratteristiche si presentino *in maniera indipendente*. Se questo presupposto è vero, allora è matematicamente legittimo e sensato utilizzare la regola del prodotto per calcolare la probabilità che a commettere il crimine sia stata *un'altra* coppia, diversa da Malcolm e Janet Collins, che per puro caso corrisponde alla descrizione degli imputati in tutte le caratteristiche considerate.

L'assunto cruciale dell'indipendenza significa che se pensiamo alle singole probabilità come a frazioni della popolazione generale, quando consideriamo tali frazioni una alla volta tutte le altre continuano a valere in sequenza. Vediamo un esempio simile con cui è un po' più facile lavorare. Supponiamo che i testimoni di un crimine abbiano affermato che il colpevole guidava una Honda Civic nera con «assetto ribassato», cioè dotata di molle speciali che fanno sì che il corpo sieda più vicino al terreno.

Ignorando il caso probabile che i testimoni abbiano identificato anche altre caratteristiche del perpetratore, supponiamo di sapere, con precisione e sulla base di dati attendibili, che nell'area di Los Angeles un'automobile su 150 è una Honda Civic nera e che una su 200 ha l'assetto ribassato. La regola del prodotto afferma che per determinare, nell'insieme complessivo delle automobili, la frazione di Honda

Civic nere con assetto ribassato, dobbiamo moltiplicare:

$$1/150 \times 1/200 = 1/30.000.$$

Ma questo calcolo si basa sul presupposto che la frazione di automobili con assetto ribassato nel caso delle Honda Civic nere sia la stessa che si ritrova nelle automobili di tutti gli altri modelli e colori. Se fosse così, potremmo dire che le caratteristiche descrittive «Honda Civic nera» e «assetto ribassato» si presentano in maniera indipendente. C'è però la possibilità che i proprietari delle Honda Civic nere richiedano di accessorizzare la vettura con molle per assetto ribassato più frequentemente dei proprietari di altre automobili. Il calcolo corretto della probabilità che un'automobile a Los Angeles sia una Honda Civic nera con assetto ribassato (supponendo di disporre di buoni dati per determinare questi numeri) deve essere svolto nel modo seguente.

Supponiamo che, nell'insieme complessivo delle automobili di Los Angeles, la frazione di Honda Civic nere sia 1 su 150 e che, tra le Honda Civic nere, quelle con assetto ribassato siano una su otto. Allora, nell'insieme complessivo delle automobili di Los Angeles, la frazione di Honda Civic nere con assetto ribassato sarà:

$$1/150 \times 1/8 = 1/(150 \times 8) = 1/1200$$

che è considerevolmente maggiore di 1/30.000.

Il numero che abbiamo qui utilizzato a titolo esemplificativo, 1/8, rappresenta la «probabilità condizionata» che un'automobile abbia l'assetto ribassato, posto che sia una Honda Civic nera. Ottenere dati attendibili per determinare quel numero, o quanto meno per darne una stima accurata, è probabilmente più difficile che stimare semplicemente la frazione di *tutte* le automobili con assetto ribassato: l'«1 su 200» del calcolo originale. Ma sicuramente, in qualunque tentativo serio - in particolare, in un processo penale -, il fatto che un numero sia difficile da determinare o stimare non è un buon motivo per assumere come punto di partenza un'ipotesi altamente dubbia quale l'indipendenza degli eventi. Il rischio di errore è aggravato quando si mette insieme un elenco di caratteristiche (sei nel caso Collins) e si presuppone che siano tutte indipendenti. Persino Charlie Eppes farebbe molta fatica a fornire i dati corretti e a elaborare una stima accurata della probabilità che una coppia che ha commesso un crimine a Los Angeles risponda a quelle sei caratteristiche.

Ma questo non fu l'unico errore commesso dalla corte originaria. Il colpo più duro che la corte suprema inferse nel suo annullamento della sentenza contro Collins riguardava un errore che (come l'assunto ingiustificato dell'indipendenza) si verifica frequentemente nell'applicazione della probabilità e della statistica ai processi penali. Tale errore viene solitamente chiamato *prosecutor's fallacy*, il sofisma dell'accusa.

Questo ragionamento capzioso consiste in una sorta di tattica di adescamento messa in atto dall'accusa, talvolta a causa di un errore involontario. D'altro canto, abbiamo il calcolo eseguito dall'avvocato dell'accusa, che nonostante la sua infondatezza, tenta di determinare il valore di:

P (corrispondenza) = la probabilità che una coppia presa a caso possieda le caratteristiche distintive in esame (uomo di colore con la barba, uomo con i baffi ecc.)

Ignorando i difetti del calcolo, e supponendo ai fini del ragionamento che P (corrispondenza) sia effettivamente uguale a 1 su 12 milioni, c'è comunque una profonda differenza tra P (corrispondenza) e

P (innocenza) = la probabilità che i Collins siano innocenti.

Come fece notare la corte suprema, nel caso Collins l'avvocato dell'accusa aveva affermato che il risultato di 1 su 12 milioni corrispondeva alla P (innocenza). Egli aveva suggerito che «poteva esserci solo una possibilità su dodici milioni che gli imputati fossero innocenti e che i veri colpevoli del furto fossero un'altra coppia con le stesse caratteristiche».

La confusione tra queste due probabilità costituisce un errore pericoloso! P (corrispondenza) cerca di calcolare la probabilità che gli imputati *siano innocenti*, ma così sfortunati da corrispondere alla descrizione dei colpevoli fornita dai testimoni. Ma come spiegarono i giudici della corte suprema, il calcolo della «probabilità di innocenza» (ammesso che una cosa del genere si possa effettivamente calcolare) deve tenere in considerazione quante altre coppie nell'area di Los Angeles possiedono le stesse sei caratteristiche. La corte affermò: «Di queste coppie, che certamente saranno poche, quale è colpevole del furto, sempre che una di esse sia colpevole?»

Mettendo a segno una stoccata magistrale che scaldò il cuore dei matematici e degli statistici di tutto il mondo quando lessero in seguito del caso Collins, i giudici aggiunsero un'appendice in cui calcolavano un'altra stima. Anche prendendo alla lettera il risultato di 1 su 12 milioni presentato dall'accusa, qual è la probabilità che da qualche parte a Los Angeles esistano almeno due coppie con le sei caratteristiche che i testimoni hanno identificato nella descrizione dei ladri? I giudici stimarono quella probabilità assumendo che esista un gran numero N di possibili colpevoli - insiemi di due persone (non necessariamente «coppie») nell'area di Los Angeles - e che ognuno abbia una probabilità di 1 su 12 milioni di rispondere alla descrizione dei ladri. Basandosi anch'essi su un presupposto di indipendenza per i diversi gruppi di due persone rispondenti alla descrizione (il che non è del tutto corretto ma non è fonte di errori sostanziali), eseguirono un calcolo utilizzando la distribuzione binomiale.

Seguendo il loro ragionamento, supponiamo di lanciare N monete, ognuna con una probabilità di 1 su 12 milioni di dare testa come risultato. Sapendo che almeno uno di questi lanci dà come risultato testa (cioè, nel nostro caso, che esiste almeno una coppia rispondente alla descrizione), qual è la probabilità che esca testa in due o più lanci, cioè che ci siano almeno due coppie che rispondono alla descrizione?

La risposta alla domanda può essere facilmente calcolata utilizzando la distribuzione binomiale (servendosi di una calcolatrice o di un foglio elettronico) e, piuttosto prevedibilmente, dipende da N : il numero di potenziali «coppie colpevoli». A titolo illustrativo, la corte ipotizzò che N fosse uguale a 12 milioni, approssimativamente il numero di persone che vivevano nell'area di Los Angeles a quell'epoca, e ottenne come risultato dei suoi calcoli «più del 40 per cento» (per la precisione, il 41,8 per cento). Data questa probabilità, i giudici affermarono che non è

affatto ragionevole concludere che gli imputati devono essere colpevoli semplicemente perché possiedono le sei caratteristiche indicate dalle descrizioni dei testimoni.

Naturalmente, scegliendo un valore differente di N si otterrebbe una risposta diversa, ma anche se N , ad esempio, fosse uguale soltanto a 3 milioni, avremmo una probabilità del 12 per cento che da qualche parte a Los Angeles esista almeno un'altra coppia che potrebbe essere considerata colpevole del furto tanto quanto i Collins, per lo meno nei termini della «dimostrazione matematica» cui si era affidato l'avvocato dell'accusa per influenzare la giuria. Sarebbe difficile affermare che tutto ciò dimostri «oltre ogni ragionevole dubbio» la colpevolezza dei Collins.

Il fatto fondamentale che la fallacia logica dell'accusa trascura è che esistono generalmente molte altre persone (o coppie), insospettate, che hanno la stessa probabilità calcolata (come 1 su 12 milioni) di possedere le caratteristiche della persona (o della coppia) sotto accusa. Pertanto, anche se gli imputati fossero innocenti, avrebbero generalmente una probabilità molto più alta della P (corrispondenza) di essere così sfortunati da corrispondere all'identikit dei perpetratori del crimine.

Il caso Collins è diventato un famoso esempio negli ambienti legali, ma non era certamente il primo caso nella storia giuridica degli Stati Uniti in cui un processo veniva deciso quasi interamente sulla base della matematica. Nel caso Collins, l'uso che venne fatto della matematica si rivelò errato. Ma le cose andarono molto diversamente in un caso altrettanto famoso risalente a un secolo prima.

Il caso del testamento Howland

Uno dei più noti casi americani di falsificazione, una *cause célèbre* nel XIX secolo, fu risolto grazie alla testimonianza cruciale di due matematici, padre e figlio. Benjamin Peirce, uno dei più grandi matematici del suo tempo, era un famoso professore a Harvard, il cui nome è tuttora usato per onorare i giovani matematici che ricevono la nomina di Benjamin Peirce Assistant Professor a Harvard. Suo figlio Charles Sanders Peirce, anch'egli uno studioso brillante, insegnava logica matematica, lavorava per la US Coast and Geodetic Survey, l'agenzia federale da cui provenivano i principali finanziamenti per la ricerca scientifica nel XIX secolo, e fu autore di prodigiose opere filosofiche che gli valsero la fama di fondatore del «pragmatismo americano».

Che genere di processo portò i Peirce a testimoniare in un'aula di tribunale in qualità di esperti? Si trattò di un caso di falsificazione riguardante il patrimonio della defunta Sylvia Ann Howland, cui era stato attribuito un valore di 2 milioni di dollari: una cifra enorme nel lontano 1865. Sua nipote, Hetty Howland Robinson, impugnò il testamento, che le lasciava solo una parte del patrimonio, sostenendo che, in base a un accordo segreto stipulato con la zia, era lei l'unica erede di tutti i suoi beni. Come prova, presentò una precedente versione del testamento della zia che non solo lasciava a lei l'intero patrimonio, ma conteneva anche una seconda pagina in cui

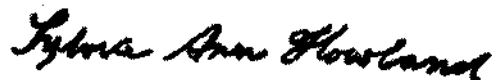
veniva dichiarato che qualunque volontà successiva doveva essere considerata priva di valore! L'esecutore testamentario, Thomas Mandell, respinse l'appello di Hetty Robinson sostenendo che la seconda pagina era un falso, e che quindi doveva essere il testamento successivo a determinare l'attribuzione dell'eredità.

Hetty Robinson non fu mai accusata del reato di falsificazione. In realtà il caso sensazionale che ne seguì, il caso *Robinson v. Mandell*, comunemente noto come il caso del testamento Howland, risultò da una causa intentata da Hetty Robinson contro la disposizione dell'esecutore testamentario! Fu questa la causa in cui si decise di fare ricorso alla matematica.

Nella maggior parte dei casi di falsificazione, qualcuno tenta di copiare la firma o la calligrafia di una persona X, e gli avvocati dell'accusa cercano di dimostrare in tribunale le differenze tra le scritte falsificate e modelli di autentica calligrafia di X. Ma in questo caso il punto era l'opposto: la falsificazione era stata fatta troppo bene!

Benjamin e Charles Peirce furono chiamati a testimoniare, a favore dell'imputato Mandell, in merito alla loro attenta analisi scientifica delle somiglianze tra la firma autentica sulla prima pagina e quella oggetto di disputa sulla seconda pagina (in realtà c'erano *due* seconde pagine, ma ne fu esaminata soltanto una):

Ecco le due firme:



Se osservate due copie della vostra stessa firma noterete subito alcune differenze. Le due firme sul testamento di Sylvia Ann Howland, invece, sembravano identiche. La spiegazione più probabile era che una fosse una ricalcatura dell'altra.

Quello che i Peirce fecero fu trasformare questo sospetto in un fatto scientifico. Essi escogitarono un metodo per confrontare ed esprimere in termini numerici il grado di accordo di qualunque coppia di firme della zia, una sorta di punteggio indicante il loro livello di uniformità. Per determinare questo punteggio, decisero di osservare i tratti discendenti - che sono trenta in ogni firma - e di contare il numero di «coincidenze» tra questi tratti nella coppia di firme esaminate. Per «coincidenza» tra due riproduzioni di un particolare tratto discendente, come quello nella prima lettera «L», essi intendevano una corrispondenza praticamente perfetta, che valutavano sovrapponendo una sull'altra le fotografie delle firme. Quando confrontarono le due firme mostrate sopra, scoprirono che tutti i trenta tratti discendenti coincidevano! Poteva trattarsi di una coincidenza puramente casuale? O questa era una chiara dimostrazione del fatto che la firma sulla seconda pagina era stata ottenuta ricalcando la firma autentica sulla prima? E qui che entrò in gioco l'analisi matematica.

I Peirce ottennero una serie di quarantadue firme sicuramente autentiche di Sylvia Ann Howland. Con quarantadue firme ci sono $42 \times 41/2 = 861$ modi di selezionare una coppia di firme da confrontare. Per ognuna di queste 861 coppie, essi determinarono il numero di coincidenze: quanti dei trenta tratti discendenti coincidevano? In tutti i 25.830 (861×30) confronti tra i tratti discendenti, i Peirce

trovarono un totale di 5325 coincidenze. Ciò significa che in circa un confronto su cinque era stata trovata una coincidenza, una corrispondenza perfetta.

Il resto della loro analisi era di natura matematica o, più precisamente, statistica. Benjamin Peirce illustrò il suo calcolo della probabilità di ottenere trenta coincidenze per trenta tratti discendenti, assumendo che la probabilità di ogni coincidenza fosse $5325/25.830 = 0,206156$. Assumendo che queste coincidenze si presentassero in maniera indipendente (!), Peirce applicò la regola del prodotto per moltiplicare tra loro le singole probabilità:

$$0,206156 \times 0,206156 \times 0,206156 \times \dots [30 \text{ volte}]$$

cioè,

$$0,206156^{30}.$$

Questa cifra equivale approssimativamente a 1 su 375.000 miliardi. (Peirce in realtà fece un errore nei suoi calcoli e ottenne un numero un po' più grande, utilizzando 2,666 al posto di 375.) Facendo sfoggio di tutta l'eloquenza che ci si aspetta da un distinto matematico del 1868, il professor Peirce riassunse le sue scoperte in questo modo: «Una improbabilità così vasta equivale praticamente a una impossibilità. Tali ombre evanescenti della probabilità non possono appartenere alla vita reale [...] La coincidenza che si è presentata qui deve avere avuto origine nell'intenzione di produrla».

Certamente non sorprende che, alla luce di un simile splendore matematico e retorico, la corte abbia deliberato contro Hetty Robinson.

Che cosa direbbe un matematico - o uno statistico - moderno dell'analisi del professor Peirce? I dati che esprimono il numero delle coincidenze sugli 861 confronti di coppie di firme possono essere analizzati per vedere quanto l'assunto dell'indipendenza sia soddisfatto, o il modello binomiale che si ottiene, e il risultato è che questi dati *non* si adattano molto bene al modello di Peirce. Ma questo non significa che la sua conclusione sull'alta improbabilità di trovare trenta coincidenze in trenta tratti discendenti non possa essere sostenuta. Come hanno messo in luce Michael O. Finkelstein e Bruce Levin parlando del caso del testamento Howland nel loro eccellente libro *Statistics for Lawyers*, oggi giorno gli statistici di solito preferiscono analizzare i dati come quelli in una maniera «non parametrica». In un'analisi di questo tipo quando vengono confrontate due firme non si parte dall'assunto che le probabilità di zero, una, due e così via fino a 30 coincidenze soddisfino qualche formula particolare o, se rappresentate in un diagramma a barre, abbiano qualche forma particolare.

Piuttosto, uno statistico dei nostri tempi preferirebbe affidarsi a un'analisi più giustificabile, come quella che afferma che se l'ipotesi nulla è vera (cioè, se la firma oggetto di disputa è autentica), allora ci sono quarantatre firme vere e $43 \times 42/2 = 903$ coppie di firme, ognuna presumibilmente con la stessa probabilità di esibire il grado massimo di accordo. Quindi, senza considerare quanto sia estremo il risultato 30 su 30, ma solo il fatto che esso rappresenta il grado più alto di accordo tra le firme di una qualunque di tutte le 903 coppie, esiste al massimo una possibilità su 903 che

quelle due firme particolari siano *più simili* delle firme di qualsiasi altra coppia. Pertanto, o si è verificato un evento molto inusuale - che ha una probabilità dieci volte più piccola dell'un per cento - oppure l'ipotesi che la firma oggetto di disputa sia autentica è falsa. Senza dubbio, Charlie Eppes lo considererebbe un motivo sufficiente per esortare suo fratello a mettere le manette a Hetty Robinson!

L'uso della matematica nella scelta dei giurati

Sospettiamo che pochi dei nostri lettori siano dei criminali. E naturalmente ci auguriamo che non siate mai stati vittima di un crimine. Quindi la maggior parte delle tecniche descritte in questo libro sarà qualcosa di cui avete semplicemente letto, o che avete visto in televisione guardando un episodio di *NUMB3RS*. Esiste però la possibilità che almeno una volta nella vostra vita veniate chiamati a far parte di una giuria (per la precisione, per i cittadini degli Stati Uniti si tratta di una possibilità su cinque).

Per molti di noi, prestare servizio in una giuria è l'unica esperienza diretta del sistema giuridico che abbiamo modo di fare in prima persona. Se dovesse capitarvi, ci sarebbe qualche possibilità che una parte delle prove che dovrete considerare sia di natura matematica. Ma assai più probabile è che, se si tratta di un caso serio, voi stessi siate inconsapevolmente oggetto di qualche analisi matematica: la matematica per la selezione delle giurie. Qui è dove gli statistici nominati dall'accusa, dalla difesa, o da entrambe - i quali oggi giorno possono sempre più avvalersi di software disponibili in commercio per l'elaborazione dei profili dei giurati - cercheranno di stabilire se avete qualche pregiudizio che potrebbe indurli a escludervi dalla giuria.

Negli Stati Uniti la nozione comune di giuria è un gruppo formato da dodici cittadini, ma le reali dimensioni delle giurie variano tra uno Stato e l'altro, e tra corti statali e federali, da un minimo di sei a un massimo di dodici membri. Sebbene siano state proposte giurie formate da soltanto tre giurati, sembra esistere un accordo generale sul fatto che sei membri sono il minimo assoluto per assicurare un livello accettabile di giustizia.²⁰

La matematica entra nella scena delle moderne giurie statunitensi all'inizio del processo di selezione, in quanto la legge federale del 1968 sulla selezione e il servizio nelle giurie autorizza «il sorteggio casuale dei nomi dei giurati dalle liste degli elettori». (Sebbene il decreto legalmente sia valido solo per le corti federali, viene solitamente preso come normativa di riferimento generale.) Come vi direbbe Charlie Eppes, quello di casualità è un concetto insidioso che richiede qualche sofisticata analisi matematica per poter essere gestito in maniera adeguata.

Uno degli obiettivi del sistema di selezione delle giurie è che i giurati costituiscano una sezione il più possibile rappresentativa della società. Pertanto, è importante che il processo di selezione - il quale, per sua natura, è soggetto al rischio di abuso - non

²⁰ Anche in Italia, i giudici popolari che affiancano i due giudici di carriera (giudici togati) nella corte d'assise e nella corte d'assise d'appello sono in numero di sei. Essi vengono sorteggiati tra i cittadini di età compresa tra i 30 e i 65 anni che godano dei diritti civili e politici e che abbiano la licenza di scuola media per la corte d'assise, e di scuola media superiore per la corte d'assise d'appello. (*N.d. T.*)

discrimini ingiustamente uno o più gruppi particolari, come le minoranze. Ma come nel caso dei pregiudizi etnici nelle operazioni di polizia (di cui abbiamo parlato nel capitolo 2), identificare le discriminazioni può essere una questione spinosa, e situazioni che all'apparenza sembrano chiari casi di discriminazione talvolta si rivelano di tutt'altra natura.

In un caso spesso citato che fu sottoposto alla corte suprema, *Castaneda v. Partida* (1977), un uomo di origini messicane, tale Rodrigo Partida, fu accusato e dichiarato colpevole di furto con intenzione di stupro in una contea al confine meridionale del Texas (Hidalgo County). Partida fece appello alla corte suprema, sostenendo che il sistema texano di selezione dei membri del gran giuri discriminava gli ispanici. Secondo i dati del censimento e i verbali dei tribunali, nel corso di un periodo di undici anni soltanto il 39 per cento delle persone chiamate a far parte dei gran giuri aveva cognomi spagnoli, mentre nella popolazione generale i cognomi spagnoli erano il 79 per cento. La corte suprema considerò questo fatto sufficiente per stabilire che si trattava di un caso *prima facie* di discriminazione.

La corte prese questa decisione basandosi su un'analisi statistica. Essa partiva dal presupposto che se i giurati venivano davvero scelti a caso dalla popolazione generale, il numero di ispanici nel campione poteva essere rappresentato attraverso il modello di una distribuzione normale. Dato che il 79,1 per cento della popolazione era costituito da messicano-americani, ci si sarebbe aspettati che il numero di ispanici tra le 870 persone chiamate a far parte dei gran giuri in quel periodo di undici anni fosse all'incirca 688. In realtà, gli ispanici convocati in quel periodo erano soltanto 339. La deviazione standard per questa distribuzione risultava all'incirca pari a dodici, il che significa che i dati osservati mostravano uno scostamento dal valore atteso di circa ventinove deviazioni standard. Dato che una differenza di due o tre deviazioni standard è di solito considerata statisticamente significativa, le cifre in questo caso erano inequivocabili. La probabilità, spesso chiamata il «valore p », che un allontanamento così sostanziale dal valore atteso si fosse verificato per caso era inferiore al su 10^{140} .

Un altro caso che fece notizia fu la sentenza pronunciata dalla corte distrettuale nel 1968 contro il famoso pediatra Benjatnin Spock, accusato di aver esortato i militari di leva a disertare durante la guerra del Vietnam. La condanna sollevò preoccupazioni quando si venne a sapere che il presunto insieme casuale di 100 persone da cui erano stati selezionati i membri della giuria comprendeva solo nove donne. Secondo i sondaggi di opinione a quell'epoca il sentimento pacifista era molto più diffuso tra le donne che tra gli uomini. Gli avvocati difensori del dottor Spock chiesero allo statistico (e professore di diritto) Hans Zeisel di esaminare la selezione delle liste dei potenziali giurati. Zeisel analizzò le 46 liste per i processi tenuti davanti ai sette giudici della corte distrettuale nei corso dei due anni e mezzo che avevano preceduto il processo contro Spock, e scoprì che le liste di uno dei giudici, quello che aveva pronunciato la sentenza nel caso Spock, comprendevano sempre un numero di donne sensibilmente inferiore rispetto alle liste degli altri giudici. Il valore p per la discrepanza in questo caso era all'incirca 1 su 10^{18} . Tuttavia, questo chiaro caso di discriminazione non fu centrale nell'annullamento della sentenza contro il dottor Spock, che fu accordato sulla base del primo emendamento.

Quello che entrambi questi casi dimostrano è come un'accurata analisi statistica possa stabilire se la selezione di una giuria coinvolge qualche discriminazione con un grado di certezza che va ben al di là della canonica soglia del «ragionevole dubbio».

Ma la selezione di una lista di giurati rappresentativa è solo una parte della storia. Il sistema giuridico americano prevede che i singoli giurati possano essere esclusi dalla lista all'inizio di un processo per tre ragioni.

La prima è che il processo sia troppo oneroso per il giurato. Di solito, questo si verifica quando è probabile che un processo duri a lungo, e possa comportare l'«isolamento» della giuria. In situazioni come queste, una madre con dei bambini piccoli, o il proprietario di una piccola impresa, ad esempio, possono chiedere di essere esonerati dal servizio. Ciò porta molti alla conclusione, non del tutto infondata, che nei processi lunghi le giurie siano costituite in gran parte da persone con molto tempo libero, come i pensionati o coloro che possono vivere con mezzi propri.

Un secondo motivo di esclusione si ha nel caso in cui uno degli avvocati riesca a dimostrare che un certo giurato non è in grado di essere imparziale in quel particolare processo.

La terza base per l'esclusione è quella che può risultare nel caso in cui un giurato venga sottoposto a un'accurata analisi statistica e psicologica. Questa è la cosiddetta rikusazione perentoria, che permette sia all'accusa sia alla difesa di escludere un certo numero di giurati senza doverne riferire le ragioni. Naturalmente, quando un avvocato chiede l'esclusione di un giurato ha sempre una ragione per farlo, cioè sospetta che quella persona non sia adatta al caso. Ma come fa a scoprirlo?

Giurie sotto esame

Sebbene il diritto alla rikusazione perentoria dia alle due parti coinvolte in un caso qualche libertà di cercare di modellare la giuria a proprio vantaggio, non dà loro il diritto di discriminare qualche gruppo protetto, come le minoranze. Nel caso del 1986 *Batson v. Kentucky*, la giuria dichiarò l'afroamericano James Batson colpevole di furto e ricettazione di beni rubati. In quel caso, l'accusa si avvalse del diritto di rikusazione perentoria per escludere dalla giuria tutti e quattro i membri afroamericani, lasciando che il caso venisse giudicato da una giuria composta soltanto da bianchi. Il caso fu rinviato al giudizio della corte suprema, la quale, basandosi sulla composizione della giuria, annullò la sentenza. All'epoca Batson stava scontando una pena di vent'anni. Piuttosto che rischiare un nuovo processo, si dichiarò colpevole di furto e fu condannato a una pena di cinque anni.

Come sempre, la sfida è stabilire quando ci si trovi effettivamente davanti a un caso di discriminazione e non a effetti dovuti a fluttuazioni casuali. In un altro caso, *United States v. Jordan*, il governo rikusò tre dei sette giurati afroamericani e soltanto tre dei ventuno giurati bianchi. Ciò significa che un afroamericano nella lista dei possibili giurati aveva una probabilità tre volte maggiore di un bianco di essere escluso dalla giuria. In questo caso il valore p risultò pari a 0,14; in altre parole, una simile selezione della giuria si verificherebbe per caso più o meno una volta su sette.

La corte d'appello decretò che non c'erano prove sufficienti per stabilire che si trattava di un caso di discriminazione.

Tuttavia, anche quando non si verificano casi di discriminazione illegale, gli avvocati dell'accusa e della difesa hanno un ampio campo di manovra per cercare di modellare a proprio vantaggio la composizione di una giuria. Il trucco è di determinare in anticipo quali caratteristiche siano indicatori affidabili del modo in cui un particolare giurato potrebbe votare. Come si fa a stabilire queste caratteristiche? Conducendo un'indagine e utilizzando la statistica per analizzare i risultati.

L'idea fu sperimentata per la prima volta all'inizio degli anni '70 dai sociologi chiamati a difendere i cosiddetti «sette di Harrisburg», attivisti pacifisti processati con l'accusa di aver tramato la distruzione degli schedari dell'organismo di arruolamento militare Selective Service System e il sequestro del segretario di Stato Henry Kissinger. La difesa basò la selezione della giuria sui dati di un'indagine locale, escludendo sistematicamente i cittadini di Harrisburg che avevano meno probabilità di simpatizzare con i dissidenti. Ben lontana dal tipo di giuria «forcaiola» che molti si aspettavano da questa città ultraconservatrice della Pennsylvania, la giuria che si pronunciò contro i sette di Harrisburg portò il processo a un punto morto per quanto riguardava le accuse più gravi e dichiarò gli attivisti colpevoli soltanto di un reato minore.

REATI AL CASINÒ

*Utilizzare la matematica per sconfiggere il sistema**Sfida a blackjack*

La croupier al tavolo del blackjack fa bene il suo lavoro. Mentre distribuisce le carte, scherza con i giocatori, sapendo che questo li incoraggerà a fare puntate sempre più alte. Un giovane con il pizzetto, i capelli lunghi e una giacca di pelle nera giunge al tavolo e prende posto. Cambia cinquemila dollari in fiches e fa un'enorme puntata sulla prossima mano. La croupier e gli altri giocatori sono sorpresi dell'entità della scommessa, ma il giovane allenta la tensione facendo qualche battuta sulla sua famiglia a Mosca. Vince la mano, guadagnando una somma considerevole, ma poi, anziché continuare a giocare, raccoglie le sue fiches e lascia il tavolo. Mentre cerca l'automobile nel parcheggio del casinò, sembra ansioso, addirittura spaventato. Qualche istante dopo un invisibile assalitore gli spara, uccidendolo.

Questa era la sequenza iniziale dell'episodio della seconda serie di *NUMB3RS* intitolato *Il segreto di Larry*, mandato in onda in Italia il 19 agosto 2007. Come spesso accade negli episodi di *NUMB3RS*, la storia non riguarda soltanto il crimine in sé, ma anche i particolari ambienti frequentati dalle vittime e dai sospetti, in questo caso il mondo dei giocatori professionisti di blackjack che sfidano i casinò. Più avanti in questo episodio gli spettatori apprendono che la vittima, Yuri Chernov, era un brillante studente di matematica a Huntington, fatto che rende il caso particolarmente adatto a Charlie. Per offrire il suo aiuto, Charlie deve prima capire le logiche dello scontro di cervelli - e talvolta non solo di cervelli - che ha caratterizzato il mondo del gioco del blackjack al casinò per oltre quarantacinque anni.

Su uno dei due fronti di questa guerra ci sono i misteriosi e furtivi «contatori di carte», spesso operanti in squadre, che applicano sofisticati calcoli matematici e capacità altamente sviluppate nei loro sforzi di ricavare grosse vincite dai casinò. Dall'altra parte ci sono i casinò, che considerano i contatori di carte degli impostori e che conservano archivi di fotografie di contatori noti. I direttori dei casinò intimano ai croupier e agli altri dipendenti di stare sempre in guardia quando vedono nuovi giocatori capaci di accaparrarsi vincite di decine di migliaia di dollari nel giro di poche ore.

Nella maggior parte degli Stati Uniti,²¹ i giocatori che contano le carte quando giocano a blackjack non sono criminali in senso letterale. Ma i casinò li vedono come avversari criminali, impostori, non diversi dai giocatori che manipolano le fiches o che cospirano con croupier disonesti per rubare il loro denaro. E a causa del rischio di essere riconosciuti ed esclusi dal gioco, i contatori di carte devono agire come

²¹ Il Nevada costituisce un'eccezione. L'alta redditività del gioco d'azzardo in questo Stato, per altri aspetti piuttosto povero, ha consentito ai casinò di fare pressioni sul potere legislativo affinché rendesse il conteggio delle carte illegale.

criminali, utilizzando travestimenti, mettendo in piedi strategie elaborate per ingannare i croupier riguardo alle loro effettive capacità, o aggirandosi furtivamente nel disperato tentativo di passare inosservati.

La causa principale delle difficoltà dei casinò è che nel blackjack, diversamente dagli altri giochi, un giocatore astuto e sufficientemente esperto può effettivamente avere un vantaggio sulla casa. I casinò realizzano un profitto - molto consistente - conoscendo le esatte probabilità di vittoria in ognuno dei loro giochi, e creando le regole in modo da avere un leggero vantaggio sui giocatori, solitamente attorno al 2-3 per cento. Questo garantisce che, sebbene uno o due giocatori possano fare un grosso colpo di tanto in tanto, la grande maggioranza dei giocatori perderà o vincerà poco, assicurando al casinò un regolare profitto settimanale o mensile.

Nel gioco di dadi chiamato *craps*, ad esempio, nessun giocatore, a meno che non ricorra effettivamente all'imbroglio (manipolando le fiches, usando dadi truccati, o compiendo qualche altra azione illegale), può vincere sul lungo termine. Quando un giocatore onesto vince, sta semplicemente compensando preventivamente le perdite che alla fine accumulerà se tornerà a giocare ancora... e ancora. La matematica garantisce che andrà a finire così.

Ma il blackjack è diverso. In determinate circostanze, i giocatori godono di un vantaggio. Un giocatore in grado di riconoscere quando la situazione è favorevole e che sa come approfittarne può, se gli viene permesso di continuare a giocare, giovare di quella percentuale di vantaggio per vincere grandi quantità di denaro. E più lo si lascia giocare, più ci si può aspettare che vinca.

Il problema del blackjack

Nei casinò, ciascun giocatore al tavolo del blackjack gioca individualmente contro il mazziere. Il giocatore e il mazziere iniziano entrambi con due carte e poi decidono a turno se prenderne un'altra. Lo scopo è totalizzare il valore più alto possibile (con le figure che valgono 10 e gli assi 1 o 11), senza «sballare», cioè senza superare 21. Se il giocatore totalizza una somma più alta del mazziere vince, se ha una somma più bassa perde. Nella maggior parte delle partite, il pagamento è alla pari, ovvero il giocatore perde la posta iniziale oppure la raddoppia.

Il punto che si è rivelato un grosso problema per i casinò è che, nella versione del gioco che offrono, il mazziere deve giocare seguendo una strategia rigida. Se il totale delle sue carte è uguale o maggiore di 17, il mazziere deve fermarsi («restare»), cioè non può più prendere un'altra carta, mentre negli altri casi è libero di scegliere se prendere un'altra carta o «restare».²² Questa regola operativa apre una piccola breccia nell'altrimenti inespugnabile muro matematico che protegge i casinò dal rischio di perdere denaro.

La possibilità di trarre vantaggio dalle regole potenzialmente favorevoli del blackjack nei casinò era nota e sfruttata soltanto da poche persone fino alla

²² Alcuni casinò applicano la cosiddetta «regola del 17 morbido», in base alla quale il mazziere deve prendere un'altra carta quando la sua somma di 17 comprende un asso contato come 11.

pubblicazione nel 1962 del libro *Beat the Dealer*, scritto da un giovane professore di matematica di nome Edward Thorp. Più o meno come Charlie Eppes - benché senza un fratello maggiore che gli chiedeva di aiutare l'FBI a risolvere i casi di crimine - Thorp stava iniziando la sua carriera come ricercatore matematico, trasferendosi dall'Università della California di Los Angeles al MIT (e in seguito all'Università della California di Irvine), quando lesse un breve articolo sul blackjack in una rivista di matematica e maturò un interesse per l'intrigante differenza tra il blackjack e gli altri giochi offerti dai casinò:

Quello che succede in un turno di gioco può influenzare quello che accadrà dopo, sia in quello stesso turno sia nei turni successivi. Il blackjack, quindi, potrebbe essere esente dalla legge matematica che vieta i sistemi di gioco d'azzardo favorevoli.²³

Le caratteristiche del gioco del blackjack che hanno effetti asimmetrici sul giocatore e sul mazziere non si limitano alla «regola del 17» per il mazziere. Il giocatore vede la prima carta del mazziere (la cosiddetta «carta scopetta») e può avvalersi di questa informazione per decidere se prendere un'altra carta o «restare», il che significa che il giocatore può impiegare una strategia variabile contro la strategia fissa del mazziere. Esistono anche altre differenze. Un'asimmetria decisamente a favore del casinò consiste nel fatto che, se il giocatore e il mazziere sballano entrambi, vince il mazziere. Altre asimmetrie, però, sono a favore del giocatore. Ad esempio, il giocatore ha la possibilità di fare giochi speciali chiamati «raddoppio» e «divisione delle coppie», che talvolta sono vantaggiosi. Un'altra regola particolarmente vantaggiosa è che se il giocatore realizza un blackjack «naturale» - cioè un asso e un 10 (o una figura) - con le prime due carte, ottiene un bonus nella forma di un pagamento 3:2 (anziché semplicemente alla pari) a meno che anche il mazziere non abbia un blackjack naturale.

I giocatori possono trarre vantaggio da queste asimmetrie perché, nel blackjack, dopo ogni mano, le carte giocate vengono scartate. Questo significa che, con il procedere del gioco, la distribuzione delle carte di valore 10 nel mazzo può cambiare, fatto di cui un giocatore astuto potrebbe approfittare per aumentare le sue probabilità di vincita.

Quando Thorp pubblicò le sue rivoluzionarie scoperte nel 1962, l'effetto netto di queste asimmetrie e di altri piccoli dettagli era che la versione del blackjack che veniva giocata a Las Vegas era essenzialmente un gioco equo, con un vantaggio per il casinò molto prossimo allo zero.

In un'industria in cui i casinò erano abituati ad avere un vantaggio assicurato, la scoperta di Thorp fu del tutto inattesa e abbastanza impressionante da fare notizia. Orde di giocatori d'azzardo si accalcarono ai tavoli del blackjack per giocare la strategia raccomandata da Thorp, la quale richiedeva di memorizzare certe regole per decidere quando prendere un'altra carta, quando fermarsi e così via, in base alla carta scoperta del mazziere. Tutte queste regole si fondavano su solidi calcoli matematici: calcoli di probabilità che, ad esempio, indicavano se un giocatore debba prendere

²³ Edward O. Thorp, *Beat the Dealer: A Winning Strategy for the Game of Twenty-One*, Random House, New York, 1962.

un'altra carta quando il totale della sua mano è 16 e la carta scoperta del mazziere è un asso. Calcolando la probabilità delle varie somme che il mazziere potrebbe totalizzare e la probabilità dei risultati che il giocatore potrebbe raggiungere prendendo un'altra carta, Thorp confrontò semplicemente le probabilità di vincere in entrambi i modi - prendendo un'altra carta e fermandosi - e suggerì ai giocatori di scegliere l'opzione migliore, in questo caso quella di prendere un'altra carta se la somma totalizzata è 16.

I casinò assistettero compiaciuti a questo considerevole aumento della loro attività, e presto si resero conto che quei nuovi fanatici del blackjack accorsi nelle sale da gioco utilizzavano la strategia di Thorp soltanto nei loro sogni. Molti aspiranti vincitori facevano fatica a ricordare tutte quelle regole sottili abbastanza bene da applicarle al momento giusto, o addirittura mostravano una mancanza di dedizione alla migliore strategia dettata dalla matematica quando si trovavano di fronte alla dura realtà della sorte. Un giro di mani buone o cattive - magari una serie di mani perdenti ottenuta seguendo una delle regole di base della strategia - spesso induceva i giocatori a non tenere più conto delle prescrizioni meticolosamente calcolate da Thorp.

Nondimeno, *Beat the Dealer* ebbe un successo straordinario, vendendo più di 700.000 copie ed entrando nella lista dei libri più venduti del *New York Times*. Il gioco del blackjack non sarebbe stato mai più lo stesso.

Contare le carte: un'arma segreta dei matematici

La strategia di base di Thorp, la prima da lui ideata, non faceva che trasformare una fonte di profitto per i casinò in un gioco equo. In che modo il blackjack divenne un gioco potenzialmente svantaggioso per i casinò e conveniente per i matematici e per i loro avidi allievi? Thorp analizzò ulteriormente la strategia del blackjack, utilizzando alcuni dei computer più potenti disponibili all'inizio degli anni '60, e sfruttò due semplici idee.

La prima è che il giocatore vari ancor di più la sua strategia (se prendere un'altra carta o fermarsi, se raddoppiare ecc.) in base alla percentuale di dieci rimasta nel mazzo. Quando le probabilità di sballare sono più alte del normale - ad esempio, quando nel mazzo rimangono molti 10 e molte figure (che valgono anch'esse dieci) e il giocatore ha una mano debole, come un 16 contro un 10 del mazziere - è ragionevole rivedere la strategia di base e decidere di fermarsi anziché prendere un'altra carta. (Se nel mazzo ci sono ancora molte carte che valgono 10, è più probabile che il giocatore, prendendo un'altra carta dopo un 16, superi 21.) D'altro canto, quando le probabilità di sballare sono inferiori alla norma - cioè quando nel mazzo rimane un numero relativamente superiore di carte basse - i giocatori possono prendere un'altra carta in situazioni in cui generalmente la strategia di base suggerirebbe loro di fermarsi. Queste modifiche trasformano il gioco equo in uno in cui il giocatore gode di un leggero vantaggio.

La seconda idea è che il giocatore modifichi la puntata sulle mani successive in base alla medesima informazione: la quantità di carte di valore 10 rimaste nel mazzo. Per quale ragione? Perché la percentuale di carte di valore 10 nel mazzo influenza le

prospettive di vittoria del giocatore nella mano successiva. Ad esempio, se nel mazzo rimangono molti 10, le probabilità di realizzare un blackjack naturale aumentano. Ovviamente, la stessa cosa vale anche per il mazziere, ma il giocatore, a differenza del mazziere, ottiene un bonus se realizza un blackjack naturale. Pertanto, una maggiore probabilità per entrambi di ottenere questo risultato implica un vantaggio netto per il giocatore!

I casinò sarebbero già stati abbastanza in difficoltà se Thorp avesse semplicemente spiegato i suoi calcoli matematici ai lettori del suo libro. Ciò li avrebbe messi alla mercé dei giocatori con capacità matematiche sufficienti per comprendere la sua analisi. Ma Thorp fece di più. Egli mostrò loro come fare a contare le carte - cioè come tenere continuamente il conto della quantità di 10 usciti rispetto alle altre carte - in modo da ottenere un indicatore utile per valutare se la prossima mano sarebbe stata più o meno favorevole della media, e in quale misura.

Il risultato fu che migliaia di lettori del libro di Thorp utilizzarono le istruzioni della sua «strategia dei dieci» per diventare contatori di carte, e copie del libro iniziarono ad apparire nelle mani dei passeggeri di treni, aerei e autobus che arrivavano a Las Vegas e in altre parti del Nevada, dove grandi quantità di denaro potevano essere vinte con l'applicazione dei risultati dell'analisi matematica di Thorp.

I casinò erano in difficoltà, e cambiarono immediatamente le regole del blackjack, rimuovendo certi aspetti del gioco che contribuivano alle possibilità di vincita dei giocatori. Introdussero anche l'uso di molteplici mazzi di carte mescolati assieme - spesso quattro, sei, o addirittura otto - e iniziarono a estrarre le carte da un portamazzi chiamato «scarpa» (*shoe*), una scatola di legno o di plastica ideata per contenere le carte mescolate e per mostrare il rovescio della carta successiva prima che venga estratta dal mazziere.

Chiamati «ferma professore» in omaggio al professor Thorp, le cui vincite personali, per quanto non enormi, furono sufficienti per accrescere ulteriormente il grande fascino del suo libro, i contenitori di mazzi multipli ebbero due effetti. In primo luogo, essi consentivano ai casinò di mescolare le carte meno frequentemente, così che senza rallentare il gioco (fatto dannoso per i profitti) potevano assicurarsi di rimescolare i mazzi quando nel contenitore rimaneva ancora un numero sostanziale di carte. Ciò impediva ai contatori di carte di sfruttare le situazioni più vantaggiose, che tendenzialmente si presentano quando rimangono relativamente poche carte da estrarre. Inoltre, il gioco con molteplici mazzi riduceva automaticamente la percentuale di vantaggio del giocatore sulla casa circa dello 0,5 per cento (principalmente a causa delle asimmetrie menzionate sopra). Un ulteriore vantaggio per il casinò era che l'estrazione da mazzi multipli mescolati assieme generalmente accresceva il tempo necessario per individuare un mazzo vantaggioso seguendo la procedura di conteggio suggerita da Thorp, e più questo tempo aumentava, maggiore era la probabilità che il giocatore facesse qualche errore nel conto.

Come prevedibile, questi cambiamenti nelle regole suscitarono proteste tra gli abituali giocatori di blackjack, i quali tuttavia si lamentavano soltanto delle ridotte possibilità di fare giochi come il «raddoppio» e la «divisione delle coppie». Alla fine i casinò cedettero e ripristinarono quelle che in sostanza erano le regole precedenti.

Ma mantennero le «scarpe» portamazzi, sebbene alcuni tavoli offrissero ancora giochi a mazzo unico.

La storia di Lorden: prima parte

A questo punto, non possiamo fare a meno di raccontare l'esperienza che uno di noi due (Lorden) ha vissuto con il sistema di Thorp. Nell'estate del 1963 ero in vacanza dall'università, ed ero tornato a casa nella California del Sud dove stavo lavorando per una compagnia aerospaziale. Rimasi affascinato dal libro di Thorp, in particolare dalla parte in cui egli spiegava come il «problema della rovina del giocatore» facesse luce sulle questioni molto pratiche delle vincite al gioco del blackjack. Avevo già avuto modo di incontrare il problema durante i miei studi al California Institute of Technology, ma non avevo mai sentito parlare del sistema di Kelly o delle altre regole di gestione del denaro spiegate da Thorp.

Ciò che queste regole riflettono è che esiste un corollario importante, ma poco compreso, del ben noto principio per cui «non si possono battere le probabilità sul lungo periodo». Molti anni dopo, in una conferenza pubblica al Caltech, dimostrai questo fatto coinvolgendo l'uditorio in un esperimento elaborato.

Programmai un computer in modo che stampasse 1100 singole «storie di gioco d'azzardo», una per ciascun membro del pubblico, che simulavano matematicamente i risultati che si potevano ottenere puntando regolarmente su un unico numero alla roulette, cinque giorni la settimana, otto ore al giorno, per un anno intero. Sebbene nel gioco della roulette il casinò abbia un vantaggio del 5,6 per cento, circa cento membri del pubblico alzarono la mano quando domandai: «Quanti di voi sono in vantaggio dopo tre mesi?» Al termine della conferenza, la donna che ottenne l'attestato incorniciato di «miglior giocatore alla roulette» aveva vinto una dura competizione. Ci furono altre tre persone nel pubblico che, come lei, avevano effettivamente realizzato un guadagno giocando alla roulette per un anno a tempo pieno! (Avendo già una certa esperienza come relatore di conferenze, prima di chiedere al computer di eseguire le simulazioni e di stampare i risultati, avevo calcolato la probabilità di non avere nessun vincitore tra i membri del pubblico, ed era accettabilmente bassa.)

Se le fluttuazioni casuali possono talvolta compensare, in un periodo di tempo così lungo, le perdite cui inevitabilmente si va incontro giocando alla roulette, allora forse non sorprende che valga anche l'opposto. Se avessi giocato a blackjack con una percentuale di vantaggio utilizzando il sistema di Thorp, avrei ancora dovuto far fronte alla possibilità di perdere le mie piccole puntate prima di raggiungere la terra promessa delle vincite a lungo termine.

Ovviamente, il libro di Thorp spiegava tutto questo e sottolineava l'utilità del sistema di Kelly, una strategia di gioco d'azzardo inventata da un fisico dei laboratori Bell negli anni '50, che insegna che non si dovrebbe mai scommettere più di una certa percentuale del proprio capitale corrente, di solito corrispondente alla percentuale media di vantaggio sul casinò. In teoria, questa strategia dovrebbe eliminare del tutto la possibilità della «rovina del giocatore». Purtroppo i giochi dei

casinò prevedono puntate minime, per cui se il vostro capitale dovesse ridursi, poniamo, a cinque dollari, non vi sarebbe consentito scommettere solo una piccola percentuale di quella cifra. Giocare un'ultima mano a quel punto vi darebbe sicuramente una buona probabilità di perdere l'intera posta: un caso autentico di rovina del giocatore.

Squadre di giocatori sfidano i casinò

La risposta iniziale dei casinò al successo del libro di Thorp si rivelò soltanto il primo round di una guerra continua tra i matematici e i casinò. Gli studiosi di matematica e delle sue proficue applicazioni presto si resero conto che il blackjack con mazzi multipli, nonostante gli ovvi svantaggi rispetto al gioco con un unico mazzo, aveva qualche caratteristica molto attraente che poteva essere sfruttata. Ad esempio, i mazzi multipli rendono più facile mascherare il conteggio delle carte, perché quando la composizione delle carte rimanenti diventa favorevole per il giocatore tende a rimanere tale, magari per diverse mani. Le fluttuazioni nel vantaggio del giocatore rispetto al mazziere sono mitigate dalla presenza di molte carte rimanenti nel mazzo.

Inoltre, i giocatori di blackjack iniziarono a giocare in squadre, un altro fatto che richiedeva i cicli di gioco molto più lunghi derivanti dall'uso di mazzi multipli. Uno dei pionieri del gioco di squadra fu Ken Uston, che lasciò il suo lavoro come vicepresidente del Pacific Stock Exchange per dedicarsi a tempo pieno alla fruttuosa attività del blackjack. Il suo libro, *Ken Uston on Blackjack*, rese popolari metodi di gioco di squadra contro i casinò che accrebbero notevolmente le possibilità dei contatori di carte di realizzare un profitto.

Nella sua forma più semplice, il gioco di squadra consiste in un gruppo di giocatori che mettono insieme il proprio denaro e condividono il ricavo netto delle loro singole vincite e perdite. Dal momento che possono volerci molte mani perché una piccola percentuale di vantaggio si traduca in vincite effettive, una squadra di, poniamo, cinque persone che agiscono come un unico giocatore può accrescere le probabilità di vincita in misura significativa, in quanto offre a ognuno la possibilità di giocare un numero di mani cinque volte maggiore rispetto a quelle che potrebbe giocare individualmente.

Inoltre, le squadre possono evitare più facilmente di essere scoperte adottando il classico principio economico della specializzazione del lavoro. Quelle che Uston propose erano «grosse squadre di giocatori», un'idea attribuita al suo mentore, un giocatore d'azzardo professionista di nome Al Francesco. L'idea consiste in questo. Il casinò può scoprire i contatori di carte perché questi hanno bisogno di modificare le dimensioni delle loro puntate, passando improvvisamente da piccole puntate, quando le probabilità sono a favore del casinò, a grosse puntate quando le carte rimanenti sono a loro favore. Ma giocando in squadra, un giocatore può evitare di essere scoperto non scommettendo nulla finché il mazzo non è sufficientemente favorevole, e poi facendo solo grosse puntate.

L'idea è che alcuni membri della squadra agiscano come «ricognitori». Il loro

compito è di giocare a diversi tavoli senza farsi notare, facendo solo piccole puntate, sempre contando le carte estratte al loro tavolo. Quando uno di loro si accorge che inizia a emergere un mazzo favorevole, manda un segnale a un altro giocatore della squadra che a quel punto giunge al tavolo e inizia a fare grosse puntate. Così il «grande scommettitore» si sposta da un tavolo all'altro facendo solo grosse puntate (e spesso accaparrando grosse vincite) e lasciando un certo tavolo quando i contatori gli segnalano che il mazzo è diventato sfavorevole. Le piccole puntate fatte dai ricognitori hanno scarsi effetti sulle vincite e perdite complessive della squadra, le quali dipendono principalmente dal grande scommettitore. Il rischio maggiore di questa strategia è che osservando gli spostamenti del grande scommettitore qualcuno potrebbe capire che cosa sta succedendo, ma nel trambusto di un casinò affollato con dozzine di tavoli del blackjack, una squadra abile ed esperta può spesso continuare ad attuare la sua strategia bene orchestrata per tutta la notte senza essere scoperta.

La possibilità di ricavare regolari profitti con questo genere di gioco di squadra iniziò a suscitare un notevole interesse tra gli studenti di matematica di diverse università. Per la maggior parte degli anni '90, squadre del MIT, in particolare, assaltarono i casinò del Nevada e di altre parti degli Stati Uniti. Le loro vincite non furono altissime (le fluttuazioni casuali hanno sempre effetti inattesi), le loro tecniche mascherate e i loro travestimenti non sempre si rivelarono efficaci, e le loro esperienze personali furono da esaltanti a orrende. Ma nel complesso ebbero la meglio sui casinò. Molti di questi episodi furono raccontati in un libro popolare, *Blackjack Club*²⁴ di Ben Mezrich, in articoli di riviste e quotidiani, in un documentario televisivo (in cui l'altro autore di questo libro, Devlin, divenne l'unico matematico ad aver recitato la parte di James Bond sullo schermo), e nel recente film *21* (che è l'altro nome con cui viene indicato il gioco del blackjack).

Ma che cosa accade oggi ai tavoli del blackjack nei casinò? Quasi sicuramente nell'ombra si aggira ancora qualche giocatore che utilizza strategie matematiche per contare le carte, ma le contromisure adottate dai casinò oggi includono macchinari ad alta tecnologia come i mescolatori di carte automatici. All'inizio degli anni '90 un camionista di nome John Breeding ebbe l'idea di sostituire la scatola portamazzi con una macchina che non solo poteva contenere molteplici mazzi ma consentiva anche di rimescolare le carte giocate nel mazzo in modo automatico e frequente. Ciò portò alla creazione delle macchine Shuffle Master, oggi visibili in molti casinò, che oltre a evitare al mazziere lo spreco di tempo dovuto alla necessità di rimescolare le carte, sottrae ai contatori di carte le loro possibilità di guadagno. La versione più recente di queste macchine, chiamata CMS (*Continuous Shuffling Machines*), approssima efficacemente un'«estrazione da un mazzo infinito», fatto che rende il conteggio delle carte del tutto inutile. Nel gergo dei giocatori professionisti di blackjack queste macchine sono soprannominate «scarpe scomode».

Esistono ancora giochi con mazzo unico, ma una fastidiosa tendenza recente dei casinò li ha trasformati in «offerte per allocchi» sostituendo il bonus di 3:2 per un blackjack naturale con uno di 6:5. Questo crea un vantaggio per il casinò ben dell'1,4 per cento, trasformando il gioco in poco più di una sana (e presumibilmente

²⁴ Trad. it. Mondadori, Milano, 2005. (N.d.T.)

dispendiosa) lezione per chi non legge tutte le postille del regolamento. (E se pensate che un vantaggio per il casinò dell'1,4 per cento non sia un granché, fareste meglio a stare lontani dai tavoli da gioco!)

L'episodio di *NUMB3RS Il segreto di Larry* si basava sull'idea che un disonesto genio della matematica fosse stato assunto come consulente per la compagnia che fabbricava le macchine mescolatrici di carte e avesse utilizzato intenzionalmente un algoritmo inadeguato per controllare il mescolamento casuale delle carte nella macchina. In seguito egli reclutò alcuni studenti di matematica e li armò delle istruzioni necessarie per decodificare gli schemi di carte distribuite dalla macchina e anticipare in tal modo la sequenza di carte che essa avrebbe estratto. Gli autori qui si valsero di una piccola licenza creativa, ma l'idea di partenza era buona. Come osserva Charlie, «nessun algoritmo matematico può generare numeri davvero casuali». Algoritmi di generazione di numeri casuali progettati male (o con lo scopo di nuocere) possono di fatto essere sfruttati, sia che appaiano nei telefoni cellulari, nella sicurezza in Internet o ai tavoli da gioco.

Nota a piè di pagina: i matematici e i giochi che scelgono di giocare

Thorp stesso non fece mai una grande fortuna con il metodo di gioco che aveva ideato, a parte quella derivante dai diritti del suo popolare libro. Ma in seguito riuscì ad arricchirsi applicando la sua esperienza matematica a un gioco diverso. Poco dopo lo straordinario successo ottenuto nella trasformazione del blackjack, rivolse l'attenzione al mercato finanziario, scrisse un libro intitolato *Beat the Market*, e costituì un fondo di copertura dei rischi al fine di utilizzare le sue idee matematiche per realizzare profitti in Borsa. Nel giro di diciannove anni, il suo fondo mostrò quello che Wall Street chiama un «rendimento netto annualizzato» del 15,1 per cento, che equivale a un po' più che raddoppiare il proprio capitale ogni cinque anni.

Oggigiorno Wall Street e le altre imprese e istituzioni finanziarie sono gremite di *quants* - persone esperte di matematica, di fisica e di materie affini - che hanno trasformato lo studio della matematica, della finanza e dell'investimento in un'impresa altamente redditizia.

Tanto per darvene un'idea.

La storia di Lorden: seconda parte

Qualche anno fa, circa dieci anni dopo la pubblicazione del libro di Thorp, feci un'esperienza che mi diede modo di capire quanto i casinò avessero preso seriamente la minaccia ai loro profitti che la matematica aveva lanciato. A quel tempo, ero tornato al Caltech come docente e la mia breve incursione da studente nel mondo dei casinò era ormai un lontano ricordo. Il mio campo di specializzazione era (ed è ancora) la statistica e la teoria della probabilità, e di tanto in tanto sentivo storie di amici di amici che vincevano grosse somme al casinò. Ero a conoscenza dei progressi nel conteggio delle carte nel blackjack che Thorp e altri avevano fatto, come il

sistema «hi-lo», in cui il giocatore tiene un unico conto continuo, aggiungendo 1 per ogni «dieci» o asso che esce dal mazzo e sottraendo 1 per ogni carta bassa (dal 2 al 6). Più il conto è in positivo, meno «dieci» o assi rimangono nel mazzo, fatto che avvantaggia il giocatore in quanto riduce le sue probabilità di sballare se prende un'altra carta dopo aver totalizzato un numero alto come 17. Queste nuove strategie erano non solo più efficaci ma anche più facili da usare dell'originaria strategia dei dieci proposta da Thorp.

Un giorno un laureando venne nel mio ufficio all'inizio del suo ultimo trimestre primaverile e mi chiese di dargli qualche lezione sulla teoria della probabilità. Voleva qualche approfondimento su alcuni argomenti (nello specifico, il modello del percorso casuale e la teoria delle fluttuazioni, per chi conosce il significato di questi termini) cui avevo solo fatto cenno nel corso ufficiale. Avrei dovuto immaginare quali erano le sue intenzioni! Dopo alcuni incontri settimanali, nei quali esaminammo insieme qualche tecnica avanzata per calcolare le probabilità e simulare certi tipi di fluttuazioni casuali, iniziai ad avere il sospetto che il suo scopo non fosse puramente matematico: «Hai qualche particolare interesse *pratico* per questi argomenti?» gli domandai.

Incoraggiato da quel piccolo incitamento, lo studente si confidò e mi raccontò alcune storie che, devo ammetterlo, suscitarono in me di riflesso un grande senso di piacere. Lui e un suo compagno, entrambi laureandi e pertanto soggetti a un carico molto limitato di lavoro in università, avevano trascorso la maggior parte delle loro giornate e serate a Las Vegas giocando a blackjack. Andavano a cercare i giochi a mazzo singolo, ancora disponibili in un ridottissimo numero di tavoli, e giocavano con poste di «quarti», cioè fiches da 25 dollari. (Il mio studente proveniva da una famiglia benestante.)

Trattandosi di due giovani che giocavano per poste molto alte, erano sottoposti a un'intensa sorveglianza e dovevano escogitare vari stratagemmi per evitare di essere scoperti ed espulsi dal gioco. Fingevano di essere ubriachi, mostravano un estremo interesse per le cameriere (questo reale), e giocavano simulando uno scarso interesse per le carte mentre tenevano segretamente i loro conti. Pianificavano gli attacchi ai casinò con notevole attenzione e astuzia.

Ogni settimana sceglievano quattro casinò e giocavano a blackjack per quattro giorni, andando a dormire in base a un piano che rendeva le giornate lunghe venti ore anziché ventiquattro: un ciclo che consentiva loro di incrociare ciascun turno di otto ore del personale del casinò solo due volte nel corso di quella settimana. La settimana successiva sceglievano altri quattro casinò, avendo cura di non ritornare mai nello stesso casinò prima che fosse passato almeno un mese.

Quello di essere espulsi dal gioco non era l'unico rischio che correvano. Come descritto nel libro di Thorp, alcuni casinò non erano alieni dall'usanza di barare facendo uso di mazzieri specializzati in tecniche come «estrarre la seconda carta», cioè dare al giocatore la *seconda* carta del mazzo nel caso in cui la prima gli assicuri un buon totale. (Per farlo, il mazziere deve sbirciare la carta in cima al mazzo ed eseguire una difficile manovra per estrarre la seconda al suo posto.) Una volta, mentre facevano le ore piccole in un casinò molto popolare e sfarzoso, il mio studente e il suo amico notarono che il cambio del mazziere al tavolo era avvenuto prima del

solito: un segnale pericoloso, secondo quanto descritto da Thorp. Giustamente diffidenti, decisero di giocare qualche altra mano e vedere che cosa succedeva.

Presto il mio studente si trovò in una situazione in cui il suo totale era 13 e la carta scoperta del mazziere era un 10, il che lo costringeva a chiedere un'altra carta. Consapevole che, il mazziere a quel punto avrebbe potuto barare, egli mantenne la calma e chiese un'altra carta. Quello che accadde dopo è degno di una scena di *NUMB3RS*. Il mazziere fece un movimento brusco con la mano per consegnare la carta richiesta, ma quello stesso movimento fece uscire dal mazzo un'altra carta che, dopo aver descritto un arco sopra il tavolo, cadde per terra. Fortunatamente, la carta che il mio studente aveva ricevuto era un 8; questo gli assicurò un totale di 21 con cui, prevedibilmente, riuscì a battere il mazziere. Con un pizzico di teatralità, questa scena insegnava tre cose: che «estraendo la seconda carta» mani inesperte potrebbero involontariamente muovere la carta in cima al mazzo in modo da svelare l'imbroglio; che la seconda carta (non vista dal mazziere baro) potrebbe risultare ancor più favorevole per il giocatore della prima; e, infine, che per i nostri eroi del Caltech era chiaramente arrivato il momento di riscuotere le loro vincite, lasciare il casinò e non farvi più ritorno.

Poche settimane dopo avermi svelato i suoi segreti, il mio studente mi disse che lui e il suo compagno avevano terminato le loro avventure a Las Vegas. Avevano realizzato un guadagno netto di 17.000 dollari - piuttosto buono a quell'epoca - e sapevano che era il momento di fermarsi. «Che cosa te lo fa pensare?» gli domandai innocentemente. Mi rispose spiegandomi come funziona il sistema di «occhi nel cielo». Sul soffitto delle sale da gioco vengono posizionate telecamere che consentono ai casinò di monitorare il gioco ai tavoli. In questo modo, essi possono scoprire non solo eventuali imbrogli ma anche i giocatori che contano le carte. Il casinò insegna agli addetti al monitoraggio del gioco come fare a contare le carte, in modo che osservando le scelte del giocatore - quando decide di aumentare o diminuire le puntate - essi possano capire con una certa sicurezza se sta contando le carte oppure no.

Una volta, il mio studente e il suo amico erano tornati a giocare in un casinò molto noto dopo un mese di assenza, utilizzando tutte le loro tecniche abituali per evitare di essere identificati come contatori di carte. Si erano seduti a un tavolo del blackjack, avevano acquistato alcuni quarti e fatto le loro puntate per la prima mano. Improvvisamente apparve un «ispettore» (capo croupier), il quale spinse le pile di fiches verso di loro e educatamente li informò che non erano più i benvenuti in quel casinò. (La legge del Nevada permette ai casinò di espellere i giocatori in modo arbitrario.)

Quando il mio studente, fingendo tutta l'innocenza di cui era capace, chiese per quale strana ragione il casinò non voleva che lui e il suo amico giocassero una semplice partita a blackjack, l'ispettore rispose: «Ci avete già portato via 700 dollari e non vi permetteremo di prendere di più». Questo un mese intero dopo l'ultima volta che erano stati lì, e soltanto per 700 dollari. Per arricchirsi i casinò dipendono dalla matematica, ma gridano «al ladro» se qualcun altro fa la stessa cosa.

APPENDICE

SINOSSI MATEMATICA DEGLI EPISODI DELLE PRIME TRE SERIE DI *NUMB3RS*

È vera la matematica di NUMB3RS?

Questa domanda ci viene rivolta molte volte. La risposta più semplice è «sì». I produttori e gli autori fanno molto per garantire che qualunque richiamo alla matematica nel programma sia corretto, facendo esaminare le idee per la sceneggiatura da uno o più matematici professionisti tra le centinaia in tutto il Paese che sono inclusi nella loro rubrica.

Una domanda cui è più difficile rispondere è se i metodi matematici rappresentati potrebbero davvero essere utilizzati per risolvere un crimine così come viene mostrato. In certi casi la risposta è un categorico «sì». Alcuni episodi sono basati su fatti veri in cui la matematica è stata effettivamente impiegata per risolvere i casi di crimine. Un paio di episodi seguono piuttosto fedelmente l'andamento di casi reali; in altri gli autori hanno forzato un po' i fatti veri introducendo elementi di fantasia per renderli più spettacolari. Ma anche quando un episodio non è basato su un caso reale, l'uso della matematica che viene rappresentato è generalmente, benché non sempre, *credibile*: potrebbe succedere. (E l'esperienza nel mondo reale ha dimostrato che anche applicazioni «incredibili» della matematica si verificano di tanto in tanto.) Lo scetticismo che alcuni critici esprimono dopo aver visto un episodio talvolta dipende dalla loro scarsa consapevolezza del potere della matematica e della vastità delle sue applicazioni.

Per molti aspetti, il miglior modo di pensare alle puntate di *NUMB3RS* è paragonarle a buoni racconti di fantascienza: in molti casi, infatti, la rappresentazione in un episodio di un determinato uso della matematica per risolvere un caso di crimine è qualcosa che, teoricamente o praticamente, potrebbe accadere in futuro.

Una cosa assolutamente non realistica sono i tempi. Nei quarantuno minuti di un episodio a ritmo serrato, Charlie deve aiutare suo fratello a risolvere il caso nell'arco di una o due «giornate televisive». Nella vita vera, l'uso della matematica nelle indagini di polizia è un processo lungo e lento. (Un'osservazione simile vale anche per le indagini della polizia scientifica rappresentate in altre serie televisive molto popolari negli Stati Uniti, come le serie *CSI*)

Un altro fatto poco realistico è che un matematico abbia familiarità con una gamma di tecniche matematiche e scientifiche così ampia come quella padroneggiata da Charlie. Ovviamente, Charlie è un supereroe televisivo, ma questo è ciò che lo rende piacevole. Osservare un vero matematico in azione non sarebbe più eccitante di guardare all'opera un vero agente dell'FBI! (Tutte le ore passate in un'automobile ad aspettare che qualcuno esca da un edificio, a esaminare i verbali o a fissare lo schermo di un computer sarebbero uno spettacolo alquanto noioso.)

Inoltre, Charlie sembra capace di raccogliere grandi masse di dati in un tempo notevolmente breve, mentre nelle reali applicazioni della matematica, trovare tutti i dati necessari e convertirli in una forma che possa essere digerita da un computer può richiedere settimane o mesi di duro lavoro. E spesso i dati di cui uno avrebbe bisogno semplicemente non sono disponibili.

Tralasciando la questione se una particolare tecnica matematica possa veramente essere utilizzata così come viene mostrato, la cosa veramente accurata e veritiera in tutti gli episodi, secondo noi, è l'*approccio* con cui Charlie affronta i problemi che Don gli pone. Egli riduce i problemi ai loro elementi essenziali, elimina ciò che è irrilevante, va alla ricerca di schemi riconoscibili, vede se esiste una tecnica matematica che possa essere applicata, magari con qualche aggiustamento, oppure - come succede in vari episodi - in assenza di un metodo direttamente applicabile determina per lo meno se esiste qualche tecnica matematica applicabile in altri casi che, per analogia, potrebbe suggerire a Don come procedere.

Ma il vero punto è un altro. L'intento di *NUMB3RS* non è quello di insegnare, o di spiegare, la matematica. Il suo scopo, che è riuscito a raggiungere con spettacolare successo, è soltanto quello di intrattenere il pubblico. Il merito dei suoi autori, ricercatori e produttori, impegnati a realizzare una delle più popolari serie poliziesche in onda sulle reti televisive statunitensi, è quello di aver fatto tutto il possibile perché la matematica fosse rappresentata correttamente. Ma dal punto di vista della buona televisione, è solo un caso che uno dei protagonisti sia un matematico. Dopotutto, la serie è rivolta a un pubblico che contiene necessariamente una percentuale molto piccola di spettatori con buone conoscenze di matematica. (Sicuramente negli Stati Uniti non ci sono undici milioni di persone - il numero medio di spettatori di un episodio di *NUMB3RS* in prima visione - con avanzate competenze matematiche!) Infatti, Nick Falacci e Cheryl Heuton, in origine creatori e ora produttori esecutivi della serie, hanno notato che quello che principalmente ha persuaso la rete televisiva a realizzare e a commercializzare il programma era il fascino di una proposta che presentava l'interazione tra due modi umanamente differenti di risolvere i problemi.

Don affronta un crimine con la logica di un poliziotto esperto, che conosce le situazioni concrete, mentre Charlie lo osserva dal punto di vista del pensiero logico astratto. Uniti da un legame familiare (sotto la soprintendenza di loro padre, Alan, interpretato da Judd Hirsch, l'unico membro del cast che davvero ha buone conoscenze di matematica avendo studiato fisica all'università), Don e Charlie lavorano insieme per risolvere i casi, dando allo spettatore un'idea di come i loro differenti approcci si intreccino e interagiscano. E su questo non sbagliano: l'interazione tra il pensiero matematico e altri approcci per risolvere i problemi è un fenomeno *molto* reale. E quello che ci ha offerto, e continua a offrirci, tutta la scienza, la tecnologia, la medicina, l'agricoltura moderna e, a dire il vero, praticamente tutte le cose da cui dipendiamo ogni giorno della nostra vita. *NUMB3RS* ha ragione da vendere.

Nelle pagine che seguono, offriamo una breve sinossi, episodio per episodio, delle prime tre serie di *NUMB3RS*. Nella maggior parte degli episodi vediamo Charlie utilizzare e fare riferimento a vari ambiti della matematica, ma nei nostri riassunti indichiamo solo il suo principale contributo alla risoluzione del caso.

PRIMA SERIE

23 gennaio 2005 - Episodio pilota 5 marzo 2006 - *Punto di origine*

Un serial killer stupratore circola per le strade di Los Angeles. Don lascia una mappa che mostra i luoghi dei delitti sul tavolo da pranzo a casa di suo padre. Per caso Charlie la vede e afferma che potrebbe aiutare a risolvere il caso impostando un'equazione matematica capace di risalire all'abitazione del killer a partire dai punti in cui sono stati ritrovati i cadaveri. Per spiegare la sua idea, fa il paragone con l'acqua spruzzata da un irrigatore da giardino: benché non sia possibile prevedere dove cadrà ogni singola goccia, se si conosce la distribuzione di tutte le gocce si può risalire al luogo in cui è posizionato l'irrigatore. Utilizzando questa equazione (che a un certo punto compare su una lavagna a casa sua), Charlie riesce a identificare una «zona calda» in cui la polizia potrà andare a raccogliere campioni di DNA al fine di rintracciare il killer.

28 gennaio 2005 - *Uncertainty Principle* 5 marzo 2006 - *Il principio di Heisenberg*

Don sta indagando su una serie di rapine in banca. Charlie utilizza l'analisi predittiva per prevedere dove i rapinatori colpiranno la prossima volta. Per spiegare il metodo, afferma che è come cercare di prevedere i movimenti di un pesce e descrive la sua soluzione come una combinazione di modelli probabilistici e analisi statistica. Ma quando Don e la sua squadra si trovano ad affrontare i ladri, avviene una grande sparatoria durante la quale perdono la vita quattro persone, compreso uno degli agenti. Charlie è distrutto e si ritira nel garage di famiglia a lavorare a un famoso problema di matematica irrisolto (il problema «P versus NP») cui anche lui ha iniziato a dedicarsi da un anno, dopo che sua madre si è ammalata gravemente. Ma Don ha bisogno dell'aiuto di suo fratello e cerca di convincere Charlie a tornare a occuparsi del caso. Quando Charlie torna a esaminare lo schema di distribuzione delle rapine nota che assomiglia a un gioco chiamato *Minesweeper*. Per scegliere l'obiettivo successivo, la banda di malviventi utilizza le informazioni raccolte durante ciascuna rapina.

4 febbraio 2005 - *Vector* 12 marzo 2008 - *Contagio*

Nell'area di Los Angeles iniziano ad ammalarsi molte persone; alcune muoiono nell'arco di ventiquattr'ore. Don e Charlie vengono chiamati indipendentemente (con sorpresa di Don) per indagare sulla possibilità di un attacco bioterroristico, cioè sull'eventualità che qualcuno abbia rilasciato un virus mortale nell'ambiente. Il funzionario del CDC (Center for Disease Control and Prevention) che ha convocato Charlie gli chiede di compiere un'«analisi vettoriale». Charlie si propone quindi di

localizzare il punto di origine del virus. Annunciando che il suo approccio coinvolge «analisi statistica a teoria dei grafi», indica tutti i casi noti su una mappa di Los Angeles, andando alla ricerca di raggruppamenti, e tenta di tracciare lo schema dell'epidemia. Successivamente spiega che sta mettendo a punto un «modello SIR» (suscettibili, infetti, risanati) della diffusione della malattia, per cercare di identificare il «paziente zero».

11 febbraio 2005 - *Structural Corruption* 12 marzo 2006 - *La forza del vento*

Uno studente universitario viene trovato morto. Il giovane sembra essersi suicidato saltando da un ponte, ma Charlie crede che sia stato ucciso, e che la sua morte sia collegata a una tesi di ingegneria a cui stava lavorando, a partire dalla quale si poteva dimostrare che la struttura di uno dei più moderni e importanti edifici di Los Angeles non era così sicura come sostenuto dal proprietario. A motivare i sospetti di Charlie è la posizione del cadavere che, in base ai suoi calcoli, contrasta con l'ipotesi che lo studente si sia gettato dal ponte. Partendo dai dati sull'edificio raccolti dal giovane, Charlie crea un modello al computer che dimostra che la sua struttura non è sicura se sottoposta a condizioni di vento insolite. Egli sospetta che il problema riguardi le fondamenta. Individuando alcuni schemi numerici nei documenti della compagnia di costruzioni, Charlie conclude che la documentazione è stata falsificata per nascondere lo sfruttamento illegale di lavoratori immigrati.

18 febbraio 2005 - *Prime Suspect* 10 giugno 2007 - *L'ipotesi di Riemann*

Una bambina di cinque anni viene rapita. Don chiede l'aiuto di Charlie quando scopre che anche il padre della bambina, Ethan, è un matematico. Quando Charlie vede i calcoli matematici che Ethan ha scribacchiato sulla lavagna dell'ufficio di casa, capisce che sta lavorando all'ipotesi di Riemann, un famoso problema di matematica che resiste a qualunque tentativo di soluzione da più di centocinquanta anni. La sua soluzione non solo procurerebbe all'artefice un premio di un milione di dollari, ma potrebbe anche fornire un metodo per violare i codici di sicurezza in Internet. Quando Don riesce a scoprire l'identità di uno dei rapitori, e apprende che il piano è di «svelare il più grande segreto finanziario del mondo», diviene chiaro perché la figlia di Ethan sia stata rapita. Ma Charlie trova un grosso errore nel ragionamento di Ethan e i due devono quindi escogitare un modo per far credere ai rapitori che egli è davvero in grado di fornire la chiave di crittografia in Internet che richiedono, e per rintracciare così il loro nascondiglio in modo da liberare la bambina.

25 febbraio 2005 - *Sabotage* 10 giugno 2007 - *Sabotaggio*

Un sabotatore si dichiara responsabile di una serie di incidenti ferroviari mortali. In ogni luogo del disastro il perpetratore lascia un messaggio numerico, affermando in una telefonata a Don che esso contiene tutto quello che c'è da sapere riguardo alla

serie di incidenti. La squadra dell'FBI presume che il messaggio sia scritto in un codice numerico, che Charlie cerca di decifrare. Sebbene riesca a individuare diversi schemi numerici nel messaggio, Charlie non è in grado di decifrarlo. Presto Charlie e la squadra dell'FBI capiscono che tutti gli incidenti sono una ricostruzione di un disastro precedente, e alla fine Charlie si rende conto che non esiste nessun codice. Il messaggio è un compendio di dati sull'incidente avvenuto anni prima. Charlie conclude dicendo: «Non è un codice ma una storia raccontata in numeri».

11 marzo 2005 - *Counterfeit Reality* 17 giugno 2007 - *Messaggi cifrati*

Una banda che vuole falsificare banconote di piccolo taglio ha preso un'artista in ostaggio per disegnare le immagini sui biglietti contraffatti. I malviventi uccidono almeno cinque persone, portando Don a credere che se l'artista sequestrata non verrà ritrovata al più presto sarà eliminata non appena terminato il suo compito. Charlie entra in scena per eseguire un algoritmo capace di migliorare la qualità delle immagini di alcune videoregistrazioni relative al caso provenienti dai circuiti di videosorveglianza. Dopo aver esaminato le banconote false, nota alcune imperfezioni che appaiono intenzionali, ma che non sembrano rivelare alcuno schema. La sua studentessa Amita gli suggerisce di osservare l'immagine da una certa angolatura, dalla quale è possibile discernere uno schema. In questo modo egli riesce a leggere un'indicazione segreta, scritta dall'artista rapita, che conduce l'FBI al luogo dove si nascondono i malviventi.

1° aprile 2005 - *Identity Crisis* 17 giugno 2007 - *Crisi d'identità*

Un uomo ricercato per frode azionaria viene trovato garrotato nel suo appartamento, e il delitto mostra misteriose somiglianze con un omicidio commesso un anno prima, un caso che Don aveva chiuso in seguito alla confessione di un ex detenuto. Temendo di aver mandato in galera un innocente, Don riapre le indagini sul vecchio caso. Chiede a Charlie di riesaminare le prove per capire se la prima volta gli sia sfuggito qualcosa. Charlie esamina le procedure di identificazione basate su fotografie o sull'esame delle impronte digitali, ed esegue un'analisi statistica dell'attendibilità delle testimonianze oculari.

15 aprile 2005 - *Sniper Zero* 17 giugno 2007 - *Nel centro del mirino*

Una serie di omicidi compiuti da un cecchino terrorizza gli abitanti di Los Angeles. All'inizio Charlie cerca di localizzare il cecchino calcolando le traiettorie dei proiettili trovati nei corpi delle vittime, dicendo di servirsi di «modelli del coefficiente di resistenza». Trasferendo i dati in un grafico e scegliendo gli assi in maniera appropriata, Charlie conclude che gli omicidi sono opera di più di un tiratore. Sospetta che i dati seguano una curva esponenziale, il che suggerisce che si tratti di un'epidemia di attacchi ispirata da un originario «cecchino zero». Paragona la situazione alla decisione di dipingere le pareti della propria casa di un determinato colore, accennando al fenomeno molto discusso del «punto critico». Analizza la

precisione dei tiratori in termini di «regressione verso la media», e conclude che lo schema chiave per individuare il cecchino zero non risiede nei luoghi dove sono state ritrovate le vittime ma in quelli da cui sono partiti i suoi spari.

22 aprile 2005 - *Dirty Bomb* 24 giugno 2007 - *Pericolo in città*

Un autocarro che trasporta materiale radioattivo viene rubato e i ladri minacciano di far esplodere una «bomba sporca» a Los Angeles entro le prossime dodici ore, a meno che non ricevano venti milioni di dollari. Mentre Don cerca di ritrovare l'autocarro, Charlie analizza i possibili schemi di dispersione delle radiazioni per arrivare a dedurre il luogo più probabile in cui la bomba potrebbe essere fatta esplodere infliggendo i maggiori danni alla popolazione. Tuttavia, a parere dell'FBI, il vero scopo della banda è quello di evacuare un'intera piazza della città, al fine di rubare preziose opere d'arte da un centro di restauro. Alla fine l'FBI riesce a identificare e a catturare i tre criminali, i quali si servono della minaccia di far esplodere la bomba per cercare di negoziare il loro rilascio. Notando che il loro comportamento durante gli interrogatori individuali ricorda un noto problema di matematica chiamato dilemma del prigioniero, Charlie riunisce i tre criminali e li mette di fronte a un calcolo di analisi del rischio, che mostra quanto ciascuno di loro perderebbe se dovesse finire in prigione. Questo induce l'uomo con la più alta perdita potenziale a confessare e a svelare dove è nascosto il materiale radioattivo.

29 aprile 2005 - *Sacrifice* 24 giugno 2007 - *L'angelo della vendetta*

Uno studioso di scienze informatiche che sta lavorando a un progetto governativo segreto viene trovato morto nella sua casa a Hollywood Hills. L'FBI scopre che alcuni dati sono stati cancellati dal computer della vittima pressappoco al momento dell'omicidio. Le indagini di Don rivelano che l'uomo stava divorziando dalla moglie e voleva evitare di darle del denaro. Utilizzando quella che egli chiama un'equazione predittiva, Charlie riesce a recuperare dal disco rigido della vittima un buon numero di dati, i quali in un primo momento sembrano suggerire che il progetto a cui l'uomo stava lavorando avesse a che fare con la statistica nel baseball. Ma eseguendo una ricerca in Internet su alcune delle sequenze di numeri, scopre che i dati non provenivano dal baseball ma da statistiche governative sugli abitanti di differenti tipi di quartieri cittadini.

6 maggio 2005 - *Noisy Edge* 1° luglio 2007 - *UFO su Los Angeles*

Insieme a un agente del National Transportation Security Board, Don indaga sulle dichiarazioni di alcuni testimoni che affermano di aver visto un oggetto misterioso volare pericolosamente vicino al centro di Los Angeles, suscitando l'allarme di un attacco terroristico. Con l'aiuto di Charlie, scoprono che in realtà si tratta di un velivolo costruito con una nuova tecnologia che potrebbe rivoluzionare l'industria aerea. Ma le indagini prendono una piega più inquietante quando il nuovo aeroplano precipita durante un volo di prova causando la morte del suo inventore, che lo stava

pilotando. Alcune testimonianze suggeriscono che si sia trattato di un sabotaggio. Si discute a lungo di un sistema, chiamato «algoritmo squish-squash», messo a punto da un matematico all'università dell'Alberta per rilevare deboli segnali (come i segnali radar) in un ambiente rumoroso.

13 maggio 2005 - *Manhunt* 1 ° luglio 2007 - *Caccia all'uomo*

Un pullman che trasporta alcuni detenuti rimane coinvolto in un incidente. Mentre Don sta svolgendo le indagini, Charlie, servendosi di un'analisi probabilistica, conclude che non si è trattato di un incidente ma di una cospirazione per liberare un pericoloso assassino, il quale intende vendicarsi uccidendo la principale testimone al suo processo. Don e Charlie devono trovarlo prima che riesca ad attuare il piano. Charlie utilizza la teoria della probabilità per prevedere gli spostamenti dell'assassino. Questo implica anche il ricorso all'analisi bayesiana per stabilire quali dei molti avvistamenti del fuggitivo riferiti dai cittadini siano più attendibili. Utilizza poi i risultati per riportare i luoghi e i tempi in un grafico in modo da fornire una traiettoria.

SECONDA SERIE

23 settembre 2005 - *Judgment Call* 8 luglio 2007 - *La vendetta*

La moglie di un giudice federale viene uccisa nel suo garage. Non è chiaro se il vero bersaglio fosse lei o suo marito, impegnato in un'udienza di un caso in cui il capo di una banda di delinquenti rischiava la pena di morte. Don vuole scoprire quale dei molti criminali che il giudice ha mandato in prigione poteva avere più ragioni per vendicarsi. Il compito di Charlie è di ridurre la lista dei possibili sospetti. All'inizio descrive il suo approccio in termini di «filtro bayesiano» e in seguito parla di «teoria della decisione al contrario». Presumibilmente quello che sta facendo è usare il teorema di Bayes «al contrario» per calcolare la probabilità che ciascun sospetto abbia commesso l'omicidio; in questo modo Don può concentrarsi solo sugli indiziati cui i calcoli di Charlie assegnano le probabilità più elevate.

30 settembre 2005 - *Better or Worse* - 8 luglio 2007 - *Il rapimento*

Una giovane donna tenta di rapinare una gioielleria di Beverly Hills mostrando al proprietario una fotografia della moglie e della figlia rapite. Mentre sta lasciando il negozio con una grande quantità di diamanti viene colpita e uccisa da una guardia di sicurezza. Charlie aiuta l'FBI decifrando il codice di apertura a distanza dell'automobile della donna, trovato nella sua borsa. Attraverso i dati dell'acquisto dell'automobile, l'FBI riesce a risalire all'identità della donna e, conseguentemente, a localizzare e a liberare la moglie e la figlia del gioielliere. Dato che la sicurezza dei codici di accesso delle automobili dipende dalla sequenza di numeri, l'approccio

matematico più «ovvio» è andare alla ricerca di schemi numerici capaci di fornire qualche indizio sull'intero codice. Questo è presumibilmente ciò che fa Charlie, anche se non specifica mai la tecnica che sta utilizzando.

7 ottobre 2005 - *Obsession* 15 luglio 2007- *La minaccia*

La moglie di un noto produttore cinematografico di Hollywood viene molestata mentre è sola in casa. L'abitazione è dotata di un complesso sistema di telecamere di sicurezza, ma nessuna è riuscita a registrare un'immagine dell'intruso. Charlie ipotizza che il molestatore conoscesse la casa e la posizione delle telecamere, e che abbia usato un laser per «accecarle» temporaneamente al momento del suo passaggio. Questo lo porta ad analizzare le videoregistrazioni utilizzando sofisticati algoritmi di ottimizzazione delle immagini capaci di generare una rappresentazione attendibile di un soggetto, in questo caso il molestatore, a partire da un numero relativamente limitato di informazioni.

14 ottobre 2005 - *Calculated Risk* 15 luglio 2007 - *La truffa del secolo*

L'episodio è chiaramente ispirato al caso Enron. La dirigente di una grande azienda produttrice di energia - che aveva denunciato una grossa truffa finanziaria - viene assassinata. Il problema che Don deve risolvere è il gran numero di persone che hanno un movente per l'omicidio: gli altri dirigenti dell'azienda che volevano evitare che la donna testimoniassero contro di loro in tribunale, le migliaia di impiegati che avrebbero perso il lavoro qualora l'azienda fosse fallita e, infine, il numero ancor più grande di persone che avrebbero perso la maggior parte della pensione. In questo caso Charlie utilizza una tecnica chiamata «algoritmo di potatura» al fine di ottenere un albero probabilistico di relazioni tra i sospetti a partire dall'insieme complessivo delle persone in qualche modo compromesse dalla frode. Elabora poi un modello del flusso di denaro nell'azienda impiegando i metodi della teoria dei fluidi al fine di identificare l'assassino.

21 ottobre 2005 - *Assassin* 22 luglio 2007 - *L'attentato*

Durante l'arresto di un falsario, Don trova un taccuino contenente alcuni dati crittografati e chiede a Charlie di aiutarlo a decifrarne il contenuto. Attingendo alle sue passate esperienze come consulente per la NSA, Charlie riesce a decifrare il codice, e scopre che il taccuino contiene i piani per l'omicidio di un esiliato colombiano vivente a Los Angeles per mano di un sicario esperto e addestrato. Il suo contributo successivo è di suggerire a Don i modi per inseguire il sicario basandosi su concetti tratti dalla teoria dei giochi, cioè su ipotesi relative a come l'assassino si comporterà in differenti situazioni.

4 novembre 2005 - *Soft Target* 22 luglio 2007 - *Gas letale*

Un'esercitazione antiterroristica del dipartimento della Sicurezza interna nella metropolitana di Los Angeles si trasforma in una vera e propria situazione di emergenza quando qualcuno libera un gas letale in uno dei treni. Don viene incaricato di risolvere il caso. Utilizzando la classica teoria della percolazione (basata sulla meccanica statistica, la quale determina il flusso di liquidi e gas sulla base del movimento delle singole molecole) per definire il flusso del gas, Charlie riesce a risalire al luogo preciso in cui è stato rilasciato. Dopo che Don ha identificato un probabile sospetto, Charlie cerca di prevedere dove e come colpirà di nuovo applicando la teoria della percolazione lineare, un campo relativamente nuovo che egli spiega facendo il paragone con i movimenti di una pallina in un flipper.

11 novembre 2005 - *Convergence* 29 luglio 2007 - *La rapina*

Una serie di furti in case di lusso di Los Angeles prende una piega più inquietante quando uno dei padroni di casa viene ucciso. I ladri sembrano disporre di una considerevole quantità di informazioni sugli oggetti di valore presenti nelle case e sugli spostamenti dei loro proprietari. Ma le case scelte come bersaglio delle rapine non sembrano avere nulla in comune, e certamente nulla che possa suggerire la fonte da cui i ladri stanno ricavando le loro informazioni. Charlie affronta il problema utilizzando tecniche di *data mining* e applicando software speciali per individuare qualche schema regolare fra tutti i furti avvenuti nella zona nel corso dei sei mesi in cui si sono verificate le rapine nelle case. Alla fine individua una serie di furti di automobili che apparentemente potrebbero essere opera della stessa banda, il che porta alla cattura dei colpevoli. Un altro contributo che egli offre è la scoperta che i ladri riuscivano a seguire gli spostamenti dei padroni di casa intercettando i segnali emessi dai chip GPS che si trovano in tutti i telefoni cellulari moderni.

18 novembre 2005 - *In Plain Sight* 29 luglio 2007 - *Sensi di colpa*

L'FBI fa irruzione in un laboratorio di metanfetamine ma la casa - in cui era stata nascosta una trappola esplosiva - salta in aria e uno degli agenti rimane ucciso. Il laboratorio era stato in parte identificato da un'analisi delle reti sociali che Charlie aveva condotto impiegando algoritmi di raggruppamento. Il tentativo di migliorare una fotografia trovata in un computer nella casa rivela un'immagine di pornografia infantile codificata con una tecnica di steganografia. Ulteriori analisi del disco rigido del computer conducono a una sezione nascosta, il cui contenuto fornisce un indizio sull'identità del capo del laboratorio.

25 novembre 2005 - *Toxin* 5 agosto 2007 - *Il negoziatore*

Un ignoto malfattore sta correggendo alcuni medicinali da banco con sostanze velenose. Questo porta Don e la sua squadra a inseguire un fuggitivo scomparso sulle montagne della California. Charlie prende ispirazione dalla teoria dell'informazione e

dal calcolo combinatorio (alberi di Steiner) per aiutare Don a risolvere il caso. Ma le applicazioni della matematica hanno qui uno spazio limitato, in quanto vengono utilizzate soltanto per dare a Don un'idea delle azioni che dovrebbe intraprendere.

9 dicembre 2005 - *Bones of Contention* 5 agosto 2007 - *Antico reperto*

In seguito al ritrovamento di un antico cranio, un'archeologa del museo viene uccisa. Charlie utilizza le sue conoscenze sulla datazione con il radiocarbonio e sui diagrammi di Voronoi (un concetto del calcolo combinatorio connesso alla distribuzione efficiente dei beni) allo scopo di aiutare a risolvere il caso. La datazione con il radiocarbonio costituisce oggi una comune tecnica matematica utilizzata per determinare l'età di scheletri e frammenti di ossa. L'accenno ai diagrammi di Voronoi è simile a quello agli alberi di Steiner nell'episodio precedente: più che altro, si tratta di un modo per concentrare l'attenzione su un aspetto chiave dell'indagine.

16 dicembre 2005 - *Scorched* 12 agosto 2007 - *Inferno sulla terra*

Un incendiario dà fuoco a una concessionaria di SUV uccidendo un commesso. Sulla scena del crimine viene trovato il nome di un gruppo di ambientalisti estremisti scritto con uno spray, ma il gruppo nega di essere coinvolto. Don deve scoprire chi sia il vero responsabile dell'incendio: il gruppo di ambientalisti o qualcun altro. Charlie viene convocato per aiutare l'FBI a capire se la distribuzione degli incendi possa in qualche modo aiutare a fornire un profilo dell'incendiario. Egli afferma di utilizzare un'«analisi delle componenti principali» per produrre «impronte» degli incendi sufficientemente precise e tali da consentire di identificare il criminale.

6 gennaio 2006 - *The O.G.* 12 agosto 2007 - *Omicidi a catena*

Un agente dell'FBI che sta lavorando sotto copertura come membro di una banda viene ucciso. Quando si scopre che la copertura non era stata smascherata, l'omicidio appare come l'ennesimo episodio nell'incessante lotta tra bande rivali. Charlie ritiene che il gran numero di omicidi nella lotta tra bande, 8000 in quattro anni, fornisca dati sufficienti per un'analisi delle reti sociali al fine di individuare catene di omicidi commessi in base a una logica *tit for tat* (occhio per occhio). L'analisi rivela diverse catene più lunghe della media, e Charlie desume che siano probabilmente opera dello stesso assassino o gruppo di assassini. Egli nota poi alcune caratteristiche insolite in certe catene, consentendo alla fine a Don di risolvere il caso. La sigla OG nel titolo originale dell'episodio sta per *old gangster* (vecchio gangster).

13 gennaio 2006 - *Doublé Down* 19 agosto 2007 - *Il segreto di Larry*

Un uomo viene ucciso subito dopo aver lasciato un casinò dove aveva vinto una somma considerevole di denaro. Quando si scopre che la vittima era un brillante studente di matematica in un'università locale, Don sospetta che facesse parte di un gruppo di giocatori che utilizzano il «conteggio delle carte» per aumentare le loro

probabilità di vincita. L'analisi di Charlie tiene conto dei più recenti sviluppi nella cinquantennale storia dell'uso di studi matematici per vincere a blackjack.

27 gennaio 2006 - *Harvest* 19 agosto 2007 - *Traffico di organi*

In seguito a una segnalazione di attività sospette nello scantinato di un albergo, Don scopre che si tratta di un caso di mercato nero degli organi. Alcune giovani donne provenienti da un'area povera della campagna indiana vengono convinte a vendere organi che verranno trapiantati in pazienti benestanti di Los Angeles. Le ragazze sono portate nello scantinato, sottoposte all'operazione e poi rimandate a casa. Dopo la morte di una di loro, Don teme che possano esserci altre vittime, in quanto la banda a questo punto non avrebbe più nulla da perdere. Il contributo di Charlie consiste nel determinare l'ora più probabile della morte della ragazza in base ad alcune fotografie di un blocco di ghiaccio parzialmente sciolto, che serviva per la conservazione di un rene asportato, scattate dalla polizia al momento dell'arrivo sulla scena del delitto.

3 febbraio 2006 - *The Running Man* 26 agosto 2007 - *Falsa identità*

Una banda di malviventi ruba un sintetizzatore di DNA dall'università in cui insegna Charlie, il CalSci, e Don sospetta che i ladri vogliano vendere la macchina a un gruppo di terroristi, che intende usarla per fabbricare armi biologiche. Charlie offre il suo aiuto (in maniera piuttosto marginale) suggerendo una possibile analogia con la legge di Benford, la quale descrive la probabilità che i numeri presenti nelle raccolte di dati reali comincino con una data cifra (1 nel 30 per cento dei casi, 2 nel 18 per cento, 3 nel 12 per cento, e così via fino a 9 soltanto nel 4 per cento dei casi). Intuitivamente si potrebbe pensare che, con una distribuzione casuale dei numeri, la probabilità che un numero inizi con una data cifra sia sempre di 1/9, ma questo non vale per i dati provenienti da fonti reali. Nel caso al quale sta lavorando Don, l'analogo della prima cifra prevalente risulta essere il laboratorio LIGO (Laser Interferometer Gravitational-Wave Observatory) del CalSci, diretto da Larry. (Il Caltech - l'equivalente del CalSci nel mondo reale - gestisce davvero un laboratorio LIGO, anche se la struttura in sé non è situata nel campus dell'università, e nemmeno in California.)

3 marzo 2006 - *Protest* 26 agosto 2007 - *Una questione in sospeso*

Don e la sua squadra stanno indagando sull'esplosione di una bomba fuori da un centro di reclutamento dell'esercito. Il caso ricorda un attentato compiuto da un attivista pacifista all'inizio degli anni '70, esattamente trentacinque anni prima, nel quale avevano perso la vita due persone. Il responsabile di quell'attentato non era mai stato catturato e il principale sospetto dell'FBI era scomparso subito dopo l'esplosione. Charlie utilizza l'analisi delle reti sociali per aiutare Don a capire chi potrebbe aver compiuto l'attentato del 1971; questo porta a un'inattesa scoperta sulle attività segrete dell'FBI nel movimento contro la guerra nel Vietnam.

10 marzo 2006 - *Mind Games* 27 agosto 2007 - *Triplo omicidio*

Seguendo gli indizi forniti da un uomo che dice di essere un sensitivo, la polizia trova i cadaveri di tre ragazze in una zona disabitata. Le vittime, tutte immigrate clandestine, sono state apparentemente uccise in bizzarre circostanze rituali, ma in seguito si scopre che sono state assassinate per recuperare droghe illegali che avevano ingerito al fine di introdurle di contrabbando nel Paese attraverso il confine con il Messico. Gran parte del lavoro di Charlie in questo episodio è dedicato a cercare di convincere Don e gli altri che i poteri paranormali non esistono e che coloro che affermano di possederli sono degli impostori. Ma egli contribuisce anche a risolvere il caso utilizzando l'equazione di Fokker-Planck (che descrive il moto caotico di un corpo soggetto a particolari forze e vincoli) per determinare dove potrebbe andare a nascondersi il prossimo gruppo di contrabbandieri.

31 marzo 2006 - *All's Fair* 27 agosto 2007 - *Delitto d'onore*

Una donna irachena, attivista politica a Los Angeles, che stava girando un documentario per promuovere i diritti delle donne musulmane, viene uccisa. Charlie esamina le raccolte di dati statistici relativi a molti possibili sospetti per cercare di individuare i colpevoli più probabili. Per fare questo, deve ponderare tutti i fattori che potrebbero indicare una volontà di uccidere. Ciò gli consente di attribuire un «punteggio» o probabilità a ciascun sospetto, e di creare una classifica in cima alla quale figurano gli indiziati principali, associati a un punteggio più alto. Una ponderazione su base statistica di questo tipo è chiamata regressione statistica, e in particolare quella utilizzata da Charlie viene definita regressione «logistica».

7 aprile 2006 - *Dark Matter* 3 settembre 2007 - *Sangue innocente*

Don e la sua squadra stanno indagando su una strage in un liceo in cui hanno perso la vita otto studenti, insieme a uno degli aggressori. La scuola è dotata di un sistema di identificazione delle frequenze radio per seguire i movimenti di tutti gli alunni nel corso della giornata, e Charlie si serve dei dati registrati dal sistema per ricostruire gli spostamenti degli aggressori e delle vittime nei corridoi della scuola, utilizzando equazioni di tipo «preda-predatore». A un certo punto la sua analisi rivela uno schema anomalo e Charlie capisce che doveva essere presente un terzo aggressore, di cui nessuno aveva sospettato in precedenza.

21 aprile 2006 - *Guns and Roses* 3 settembre 2007 - *Omicidio o suicidio?*

Un'agente della polizia governativa viene trovata morta nella sua casa. All'inizio tutto fa pensare a un suicidio, ma quando cominciano a emergere i dettagli sulle indagini recenti e sulla vita privata della donna, Don inizia a sospettare che qualcuno l'abbia uccisa. Charlie utilizza la tecnica delle «impronte acustiche», basandosi su registrazioni del colpo d'arma da fuoco captate dalle radio della polizia nella zona, e

conclude che al momento della morte della donna doveva esserci un'altra persona nella stanza. Questa tecnica è stata impiegata in diversi casi di sparatorie reali, compreso quello dell'assassinio di Kennedy nel 1963, dove l'analisi matematica aveva indicato la probabile presenza di un secondo tiratore sul famigerato «colle erboso».

28 aprile 2006 - *Rampage* 10 settembre 2007 - *Attacco all'FBI*

Un uomo ruba una pistola a un agente negli uffici dell'FBI e inizia a sparare all'impazzata. Dopo che l'agente David Sinclair riesce a fermarlo, si scopre che l'uomo è un rispettabile marito e padre di famiglia, apparentemente privo di un movente. Dopo molte indagini, Don apprende che l'uomo era una pedina in un elaborato piano volto a far deragliare l'imminente processo contro un pericoloso trafficante di armi. Charlie offre un contributo fondamentale alle indagini dimostrando che i movimenti dell'aggressore si avvicinavano molto al modello del moto browniano (casuale). Utilizza anche un'analogia con un ipercubo a quattro dimensioni per motivare un'analisi della sparatoria dal punto di vista di un evento spaziotemporale.

5 maggio 2006 - *Backscatter* 10 settembre 2007 - *Frode su Internet*

Don sta indagando su una frode informatica che ha preso come bersaglio il sistema di dati di una banca per avere accesso alle informazioni sull'identità e sul patrimonio finanziario dei suoi clienti, tra cui lo stesso Don. Si scopre che dietro all'attività si cela la mafia russa. Stranamente, sebbene la sicurezza dei computer e dei sistemi di dati delle banche dipenda da un gran numero di tecniche matematiche avanzate, alcune delle quali menzionate da Charlie, il caso viene risolto senza un sostanziale intervento della matematica: tutto è implicito, celato nei sistemi che Charlie e Amita utilizzano per aiutare Don a rintracciare i criminali.

12 maggio 2006 - *Undercurrents* 17 settembre 2007 - *Influenza aviaria*

I corpi di diverse ragazze asiatiche, che probabilmente erano stati gettati nel mare, vengono ritrovati sulla spiaggia, portati a riva dalla corrente. La situazione diviene più critica quando si scopre la presenza del virus dell'influenza aviaria in una delle ragazze. Charlie esegue alcuni calcoli sulle correnti oceaniche per determinare il luogo più probabile in cui le vittime sono entrate in acqua. Con il procedere delle indagini, Don e la sua squadra scoprono una connessione tra le ragazze morte e il mercato della prostituzione.

19 maggio 2006 - *Hot Shot* 17 settembre 2007 - *Serial killer*

Don sta indagando sugli omicidi di due giovani donne, trovate morte ognuna nella propria automobile parcheggiata davanti alla sua casa. Qualcuno aveva fatto in modo che le morti sembrassero causate da un'overdose di stupefacenti, ma Don arriva

presto a concludere che si tratta di omicidi perpetrati da un serial killer. Charlie cerca di aiutare a risolvere il caso analizzando la routine quotidiana delle due donne, e andando alla ricerca di schemi regolari che potrebbero condurre all'identità del killer, ma Don risolve il caso in gran parte per mezzo delle ordinarie tecniche investigative.

TERZA SERIE

(i titoli degli episodi in italiano e le date di trasmissione, sono a cura dei Bluebook)

22 settembre 2006 - Spree 30 Giugno 2008 - Le strade del destino

È la prima parte di un episodio in due puntate. Una giovane coppia è protagonista di una folle serie di rapine e omicidi in tutto il Paese. Quando diviene chiaro che i loro spostamenti sono influenzati da quelli di un agente dell'FBI che li sta inseguendo, collaborando con Don e la sua squadra, Charlie utilizza le «curve di inseguimento» per aiutare l'FBI a rintracciare la coppia di criminali. Ma l'efficacia dei metodi matematici impiegati diviene incerta dopo che l'uomo viene catturato e la donna prende in ostaggio l'agente Reeves per negoziare il rilascio del suo compagno.

29 settembre 2006 - Two Daughters 30 giugno 2008 - L'ostaggio

È la continuazione dell'episodio precedente.

6 ottobre 2006 - Provenance 6 luglio 2008 - Il furto

Un ladro ruba un quadro di valore in una piccola galleria d'arte locale. Il caso prende una piega più sinistra quando uno dei principali sospetti viene ucciso. Charlie analizza una fotografia ad alta risoluzione del dipinto scomparso facendo uso di tecniche matematiche e, confrontando i suoi risultati con un'analisi simile di altri quadri dello stesso artista, conclude che il quadro rubato è un falso, il che porta Don a rivedere la lista dei sospetti. L'analisi di Charlie impiega un metodo messo a punto da un (vero) matematico al Dartmouth College, che riduce i particolari di un quadro (zone di luce e ombra, scelta dei colori, prospettiva e forme utilizzate, profondità, spessore e direzione delle pennellate, forme e solchi tra le pennellate ecc.) a una serie di numeri: una sorta di «impronta digitale» numerica della tecnica del pittore.

13 ottobre 2006 - The Mole 6 luglio 2008 - La talpa

Un'interprete del consolato cinese viene uccisa da un pirata della strada. Quando Charlie esegue un'analisi matematica sul modo in cui deve essere avvenuto l'urto, diviene chiaro che la donna è stata uccisa. Compiendo alcune indagini sulla vittima, Don scopre che era probabilmente una spia. Sebbene Charlie offra il proprio contributo utilizzando un algoritmo di riconoscimento facciale che ha messo a punto, nonché impiegando algoritmi di estrazione di dati steganografati per rivelare messaggi nascosti nelle immagini digitali, Don e la sua squadra risolvono il caso in gran parte senza l'aiuto di Charlie, utilizzando tecniche non matematiche più tradizionali.

20 ottobre 2006 - *Traffic* 7 luglio 2008 - *Il killer dell'autostrada*

Don sta indagando su una serie di aggressioni sulle autostrade di Los Angeles. Si tratta di coincidenze o dell'opera di un unico aggressore? È possibile che alcuni di questi episodi siano imitazioni di altri? In un primo momento Charlie e Amita analizzano il flusso di traffico utilizzando i modelli matematici che descrivono il movimento dei fluidi, frequentemente utilizzati anche negli studi reali sull'andamento del traffico. Ma il principale contributo di Charlie giunge quando viene suggerito che le caratteristiche delle aggressioni e le scelte delle vittime sembrano troppo casuali. Egli esamina lo schema di distribuzione dei criminali e convince Don del fatto che devono essere opera di un unico aggressore. A questo punto la sfida è trovare il fattore nascosto che accomuna tutte le vittime.

27 ottobre 2006 - *Longshot* 7 luglio 2008 - *Febbre da cavallo*

Questo è uno dei pochi episodi di *NUMB3RS* in cui non viene fatto buon uso della matematica. Un giocatore abituale alle corse di cavalli viene ucciso all'ippodromo. Si scopre che negli ultimi cinque giorni l'uomo aveva fatto trenta scommesse su trenta corse, vincendo sempre. Questo è un evento talmente improbabile dal punto di vista matematico da suggerire che tutte le corse dovevano essere truccate; eppure Charlie, che di solito non sbaglia nei suoi ragionamenti matematici, sembra non notarlo. Se lo avesse fatto, Don, che ragiona sempre dal punto di vista della conoscenza pratica e realistica del mondo, certamente avrebbe sostenuto che nemmeno una banda organizzata di criminali poteva truccare così tante corse. In tutto e per tutto, da una prospettiva matematica e in termini di credibilità, l'episodio è un fiasco. E con questo abbiamo detto tutto.

3 novembre 2006 - *Blackout* 13 luglio 2008 - *Blackout*

Una serie di interruzioni di corrente in alcune sottostazioni elettriche causa dei blackout in alcune zone di Los Angeles. Don teme che un gruppo di terroristi stia facendo delle prove prima di lanciare un attacco per provocare interruzioni di corrente a cascata che faranno piombare nel buio l'intera città. Ma quando Charlie analizza la rete di flusso, scopre che nessuna delle sottostazioni colpite potrebbe innescare simili effetti a catena, e inizia quindi a sospettare che gli attacchi abbiano uno scopo diverso. Analizzando sia le sottostazioni colpite sia quelle non colpite attraverso la teoria elementare degli insiemi (diagrammi di Venn e combinazioni booleane), egli riesce a identificare il vero bersaglio: una prigione in cui è rinchiuso un uomo in attesa di giudizio, che molti altri criminali preferirebbero vedere morto.

10 novembre 2006 - *Hardball* 13 luglio 2008 - *Baseball*

Un anziano giocatore di baseball muore improvvisamente durante un allenamento. Il caso rivela un lato inquietante quando si scopre, frugando nel suo armadietto, che è rimasto vittima di una dose di steroidi deliberatamente calcolata per ucciderlo. Charlie entra in scena quando viene scoperta una serie di e-mail che sembrano essere state inviate al giocatore ucciso con lo scopo di ricattarlo. Il motivo per cui diviene

importante il contributo di Charlie è che l'ignoto autore delle e-mail basava le sue accuse su un'analisi matematica delle prestazioni del giocatore, dalla quale si poteva desumere esattamente quando avesse iniziato a fare uso di steroidi. I primi sospetti cadono su un giovane appassionato di baseball che si serve della sabermetrica (l'analisi matematica dei dati statistici sulle prestazioni nel baseball) per giocare a fantabaseball. La principale nozione matematica che aveva permesso al giovane di capire che il giocatore stava facendo uso di steroidi è chiamata individuazione dei punti di cambiamento.

17 novembre 2006 - *Waste Not* 14 luglio 2008 - *Rifiuti*

Un improvviso sprofondamento del terreno nel cortile di una scuola causa la morte di un adulto e il ferimento di diversi bambini. Don viene incaricato di svolgere alcune indagini sulla compagnia costruttrice, già indagata per sospetta negligenza. Charlie analizza i bollettini sanitari nella regione di Los Angeles e nota un'incidenza insolitamente elevata di cancro e altre malattie nei bambini abitanti in aree in cui la compagnia aveva costruito un campo giochi, servendosi di un sostituto dell'asfalto ottenuto da rifiuti tossici riciclati. Il materiale sembra innocuo, ma quando Charlie nota una discrepanza tra il materiale di scarto mandato alla compagnia e quello prodotto per coprire la superficie dei campi da gioco, sorge in lui il sospetto che bidoni di materiale tossico non trattati siano stati seppelliti sotto i campi da gioco. Charlie si serve di tecniche di sismologia a riflessione per localizzare alcuni dei bidoni sepolti. Si tratta di un metodo per ottenere un'immagine del terreno al di sotto della superficie analizzando matematicamente la riflessione delle onde d'urto prodotte da piccole esplosioni sotterranee...

24 novembre 2006 - *Brutus* 14 luglio 2008 - *Progetto Brutus*

Un senatore dello Stato della California e uno psichiatra vengono uccisi. I due casi sembrano molto diversi, ma Don crede che siano collegati. Il contributo di Charlie consiste nell'utilizzare la teoria delle reti per svelare le possibili connessioni tra le due vittime. La pista seguita conduce a fatti tenuti segreti dal governo da molto tempo. All'inizio dell'episodio Charlie sperimenta un sistema di sorveglianza delle folle che ha messo a punto basandosi sulle teorie matematiche del flusso dei fluidi.

15 dicembre 2006 - *Killer Chat* 20 luglio 2008 - *Buon viaggio Larry!*

Charlie aiuta Don a trovare un assassino che ha ucciso diversi maniaci sessuali. I maniaci assassinati avevano tutti approfittato di ragazze minorenni che avevano incontrato in chat room online e si scopre che chi li ha uccisi li aveva adescati in Internet fingendo di essere un'adolescente. Il principale contributo di Charlie consiste nell'analizzare gli schemi linguistici dei vari partecipanti alla chat, tratti dai registri, una tecnica che viene spesso utilizzata anche nelle reali operazioni di polizia.

5 gennaio 2007 - *Nine Wives* - 20 luglio 2008 - *Il profeta*

Don, Charlie e la squadra dell'FBI sono alla ricerca di un poligamo in fuga. L'uomo, colpevole di stupro e omicidio, figura nella lista dei primi dieci ricercati

dall'FBI. Gli eventi di questo episodio riflettono piuttosto fedelmente quelli del caso vero di Warren Steed Jeffs, e la setta fittizia delle «nove mogli» si ispira alla FLDS (Fundamentalist Church of Jesus Christ of Latter Day Saints) di cui Jeffs era il capo. Il principale contributo offerto da Charlie consiste nell'analisi di un diagramma di rete trovato in uno dei nascondigli della setta, che la direttrice del suo dipartimento, Millie, identifica come un grafo di discendenza genetica.

12 gennaio 2007 - *Finders Keepers* 27 luglio 2008 - *Il relitto*

Quando un costoso yacht da competizione affonda nel bel mezzo di una regata, Don non è l'unico a essere coinvolto. Sulla scena giungono anche agenti della National Security Agency. Charlie fornisce il suo aiuto utilizzando equazioni di dinamica dei fluidi per calcolare il luogo più probabile in cui potrebbe trovarsi l'imbarcazione. Quando alla fine essa viene ritrovata da un'altra parte, diviene chiaro che la vicenda è molto più complessa di quanto sia apparso inizialmente. Charlie compie un'ulteriore analisi del tragitto dello yacht e conclude che esso doveva trasportare un pesante carico nascosto nella carena. A questo punto gli agenti della NSA sono costretti a svelare le ragioni del loro coinvolgimento.

2 febbraio 2007 - *Take Out* 27 luglio 2008 - *Senza pietà*

Una banda di malviventi ha derubato alcuni clienti di ristoranti di lusso, causando anche la morte di alcune persone. Charlie analizza lo schema di distribuzione dei ristoranti per cercare di capire quale sarà il bersaglio più probabile del loro prossimo colpo. Quando la banda assalta un altro ristorante, assente nella lista di Charlie, egli deve rivedere i presupposti della sua analisi. Presto diviene chiaro che i furti non hanno come unico scopo quello di rubare denaro. Per rintracciare i criminali, Charlie deve trovare un modo per seguire il flusso di capitali attraverso banche estere che operano il riciclaggio di denaro sporco.

9 febbraio 2007 - *End of Watch* 3 agosto 2008 - *Vivere o morire*

Don e la sua squadra riaprono un vecchio caso irrisolto quando un distintivo della polizia di Los Angeles viene ritrovato in un cantiere. Charlie impiega una tecnica molto sofisticata (e matematicamente complessa), chiamata LSM (*Laser Swath Mapping*), per localizzare i resti sepolti del proprietario del distintivo, un agente di polizia scomparso diciassette anni prima. Questa tecnica di telerilevamento utilizza un raggio laser altamente concentrato proveniente da un aereo a bassa quota per identificare ondulazioni nel terreno. In seguito Charlie impiega l'analisi dei sentieri causali per cercare di ricostruire le azioni dell'agente il giorno della sua morte. Il titolo originale dell'episodio, *End of Watch*, è un modo di dire della polizia statunitense che indica la morte di un poliziotto. Ai funerali, l'espressione viene utilizzata per indicare la data di morte degli agenti.

16 febbraio 2007 - *Contenders* 3 agosto 2008 - *Morte sul ring*

Un vecchio amico di scuola di David uccide un avversario sul ring durante un allenamento di pugilato. Tutto fa pensare a un incidente finché non si scopre che la stessa cosa è già accaduta in passato. Quando il coroner scopre che il pugile morto era stato avvelenato, le cose si mettono male per l'amico di David, ma un'analisi del DNA condotta su alcune prove chiave alla fine lo scagiona. Charlie dice di poter usare una «variante del conteggio di Kruskal» per esaminare le serie di incontri combattuti dai pugili morti in modo da risalire all'identità del probabile assassino. Il conteggio di Kruskal è un metodo usato dai prestigiatori per tenere il conto delle carte da gioco e «prevedere» il valore di una carta che apparentemente si è persa in una serie di mescolamenti. È difficile capire come questa tecnica potrebbe essere utilizzata nel modo suggerito da Charlie. Forse era stato distratto dalla sua imminente partecipazione a un campionato di poker, che rappresenta il secondo tema di questo episodio.

23 febbraio 2007 - *One Hour* 10 agosto 2008 - *Il labirinto*

Mentre Don è occupato a parlare con il suo psichiatra, la sua squadra ingaggia una lotta contro il tempo per trovare un bambino di undici anni, figlio di un ricco gangster locale, che è stato rapito con una richiesta di riscatto di tre milioni di dollari. Gran parte dell'azione si concentra sul percorso tortuoso che i rapitori fanno seguire all'agente Colby Granger per le strade di Los Angeles in modo da seminare qualunque potenziale pedinatore, una scena tratta dal film con Clint Eastwood *Ispettore Callaghan: il caso Scorpion è tuo*. Charlie e Amita cercano di capire la logica dietro il tragitto che i rapitori fanno percorrere a Colby, anche se non viene mai esplicitato in che modo. Considerato il numero relativamente limitato di dati disponibili, sembra improbabile che possano riuscire nell'impresa.

9 marzo 2007 - *Democracy* 10 agosto 2008 - *Potere e denaro*

Una serie di omicidi commessi a Los Angeles sembra avere a che fare con una frode elettorale compiuta utilizzando sistemi elettronici di voto. Don, Charlie e la squadra dell'FBI devono trovare l'assassino prima che colpisca di nuovo. Sebbene la sicurezza dei sistemi elettronici di voto coinvolga molte tecniche matematiche avanzate, il principale contributo di Charlie alla soluzione del caso è proprio all'inizio, quando calcola la probabilità che una determinata serie di morti sia accidentale. Scoprendo che questa probabilità è estremamente bassa, Don si convince del fatto che siano tutti casi di omicidio.

30 marzo 2007 - *Pandora's Box* 17 agosto 2008 - *Doppia indagine*

Un jet privato precipita nella foresta mentre una guardia forestale assiste alla scena. Quando l'uomo va a indagare sull'accaduto viene ucciso, il che fa sorgere il sospetto di un sabotaggio. La scatola nera viene recuperata ed esaminata (da Charlie in un

laboratorio del CalSci) e si scopre che i dati registrati indicano una quota di volo molto superiore a quella effettiva al momento dell'incidente. Esaminando l'area in cui sono stati ritrovati i rottami, Charlie riesce a localizzare il computer per il controllo di volo dell'aereo. Quando analizza il codice, scopre che l'incidente era uno stratagemma per fare in modo che esso venisse inserito nel computer di controllo principale dell'aviazione civile al momento della lettura della scatola nera. L'altro importante contributo di Charlie alla risoluzione del caso consiste nell'uso di tecniche di ottimizzazione delle immagini per migliorare la qualità di alcune impronte digitali indistinte.

6 aprile 2007 - *Burn Rate* 17 agosto 2008 - *Lettere esplosive*

Una serie di lettere esplosive inviate come gesto di protesta contro la ricerca biotecnologica ha le stesse caratteristiche di una serie precedente per cui qualcuno sta già scontando una pena in carcere. Il primo contributo di Charlie consiste nell'analizzare i frantumi lasciati dalle esplosioni per stabilire come sono state costruite le bombe. Successivamente egli osserva la distribuzione degli indirizzi da cui sono state spedite le bombe per limitare la gamma dei luoghi in cui è probabile che risieda il sospetto principale. Ma quando si rende conto che i dati sono tutti troppo coerenti - nessuno cade troppo lontano dagli altri - capisce che il colpevole non può essere la persona che Don sospetta. Ma chi è allora?

27 aprile 2007 - *The Art of Reckoning* 24 agosto 2008 - *La macchina della verità*

Un sicario condannato a morte si pente e accetta di confessare i propri reati in cambio della possibilità di rivedere sua figlia prima di essere giustiziato. Charlie consiglia a Don come condurre la trattativa spiegando la strategia *tit for tat* nelle serie ripetute di sfide tra due giocatori rivali nel gioco del dilemma del prigioniero. L'uso della risonanza magnetica funzionale per stabilire se il condannato stia dicendo o meno la verità dipende da molti studi matematici sofisticati, ma, essendo questi parte integrante della stessa tecnologia, Charlie non deve esplicitarli.

4 maggio 2007 - *Under Pressure* 24 agosto 2008 - *Sotto pressione*

Le informazioni recuperate da un computer portatile ritrovato nello Yemen indicano che una banda di terroristi intende pompare del gas nervino negli acquedotti di Los Angeles. Charlie utilizza un'analisi di rete per cercare di capire chi potrebbero essere i principali soggetti coinvolti. Charlie offre la maggior parte del suo contributo prima che l'episodio abbia inizio.

11 maggio 2007 - *Money for Nothing* 31 agosto 2008 - *Progetto Zambia*

Un autocarro che trasporta medicinali e cinquanta milioni di dollari in contanti destinati a un piano di soccorso in Africa viene dirottato da una banda di ladri ben

informati. I tentativi dell'FBI di localizzare la partita vengono intralciati dalle azioni dei cacciatori di taglie. Charlie esegue un'analisi matematica delle possibili vie di fuga seguite dall'autocarro.

18 maggio 2007 - *The Janus List* 31 agosto 2008 - *Messaggio in codice*

Un ex crittologo per i servizi segreti britannici affronta l'FBI e causa una serie di violente esplosioni su un ponte; le sue azioni fanno parte di un piano disperato volto a smascherare le «spie doppie» che lo hanno avvelenato. Per aiutare l'FBI a seguire la complicata pista indicata dal crittologo e a creare i contatti necessari per ottenere la lista dei doppiogiochisti, Charlie deve decifrare messaggi che sono stati codificati utilizzando una molteplicità di tecniche, compreso lo *straddling checkerboard* e un sistema di crittografia musicale.

RINGRAZIAMENTI

Desideriamo ringraziare gli autori di *NUMB3RS*, Cheryl Heuton e Nick Falacci, per aver creato Charlie Eppes, il primo matematico a diventare un supereroe della televisione, e soprattutto per essere riusciti brillantemente nell'impresa di rappresentare la matematica in prima serata. Al loro sforzo si è unito un gruppo straordinario di altri autori, attori, produttori, direttori e specialisti il cui lavoro è stato la fonte di ispirazione per questo libro. Il bravo attore David Krumholtz si è guadagnato ovunque l'eterna riconoscenza dei matematici per aver dato vita a Charlie in un modo che ha portato milioni di persone a vedere la matematica sotto una luce completamente nuova. Ringraziamo anche i ricercatori di *NUMB3RS*, Andy Black e Matt Kolokoff, per il meraviglioso lavoro che hanno fatto trovando un numero sterminato di applicazioni della matematica e facendo così avverare i sogni degli autori.

Desideriamo rivolgere un ringraziamento particolare al matematico Lenny Rudin della Cognitech, uno dei maggiori esperti al mondo di tecniche di ottimizzazione delle immagini, per il suo fondamentale contributo nel capitolo 5, sia per il contenuto, sia per le immagini.

Infine il nostro agente, Ted Weinstein, ci ha trovato un ottimo editore, David Cashion della Piume, ed entrambi hanno lavorato instancabilmente per trasformare un'opera che a nostro parere era quanto di più vicino al lettore si potesse chiedere a un libro di matematica in una che, dobbiamo ammetterlo, ora lo è molto di più!

*Keith Devlin, Palo Alto,
CA Gary Lorden, Pasadena, CA*

CREDITI DELLE ILLUSTRAZIONI

[Figura 7](#): per gentile concessione degli autori.

[Figura 9](#): per gentile concessione di Valdis Krebs, www.orgnet.com.

[Nodi](#): per gentile concessione di Gary Lorden.

[Esperimento Hong Kong](#): per gentile concessione di Lawrence M. Wein, Stanford University.